

# Dell PowerEdge FN I/O Module

Command Line Reference Guide

9.14.1.5

## Notes, cautions, and warnings

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

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

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

<b>Chapter 1: About this Guide</b> .....	<b>43</b>
Objectives.....	43
Audience.....	43
Conventions.....	43
Information Icons.....	44
<b>Chapter 2: Before You Start</b> .....	<b>45</b>
Operational Modes.....	45
Default Settings.....	45
Other Auto-Configured Settings.....	46
DCB Support.....	46
FCoE Connectivity.....	46
iSCSI Operation.....	46
Link Aggregation.....	47
Uplink Failure Detection.....	47
VLANs.....	47
Where to Go From Here.....	48
<b>Chapter 3: CLI Basics</b> .....	<b>49</b>
Accessing the Command Line.....	49
Multiple Configuration Users.....	49
Navigating the CLI.....	50
Obtaining Help.....	50
Using the Keyword no Command.....	51
Filtering show Commands.....	52
Command Modes.....	53
Track Login Activity.....	54
Restrictions for Tracking Login Activity.....	54
Configuring Login Activity Tracking.....	54
Display Login Statistics.....	55
Limit Concurrent Login Sessions.....	56
Restrictions for Limiting the Number of Concurrent Sessions.....	56
Configuring Concurrent Session Limit.....	56
Enabling the System to Clear Existing Sessions.....	56
<b>Chapter 4: File Management</b> .....	<b>58</b>
boot system gateway.....	58
boot system stack-unit.....	59
cd.....	59
copy.....	59
copy running-config startup-config.....	61
delete.....	61
dir.....	62
format flash.....	62

HTTP Copy via CLI.....	63
logging coredump stack-unit.....	63
logging coredump server.....	64
pwd.....	64
rename.....	65
restore factory-defaults.....	65
show boot system.....	67
show file.....	67
show file-systems.....	68
show os-version.....	69
show running-config.....	69
show startup-config.....	71
show version.....	71
upgrade boot.....	72
upgrade system.....	73
verify.....	74
<b>Chapter 5: Control and Monitoring.....</b>	<b>76</b>
asf-mode.....	77
asset-tag.....	77
banner exec.....	78
banner login.....	79
banner motd.....	80
clear alarms.....	80
clear command history.....	81
clear line.....	81
configure.....	81
debug cpu-traffic-stats.....	82
debug ifm trace-flags.....	82
debug ftpserver.....	83
disable.....	83
do.....	83
enable.....	84
exec-banner.....	85
enable optic-info-update interval.....	85
enable secure.....	85
end.....	86
exec-timeout.....	86
exit.....	87
feature unique-name.....	87
ftp-server enable.....	88
ftp-server topdir.....	88
ftp-server username.....	89
hostname.....	89
http-server.....	90
ip ftp password.....	90
ip ftp source-interface.....	91
ip telnet server enable.....	91
ip telnet source-interface.....	92
ip ftp username.....	92



line.....	92
login concurrent-session.....	93
login statistics.....	94
motd-banner.....	96
show login statistics.....	96
show software ifm.....	98
ping.....	99
reload.....	100
service timestamps.....	100
show alarms.....	101
show command-history.....	102
show configuration lock.....	103
show cpu-traffic-stats.....	104
show debugging.....	104
show diag.....	105
show environment.....	105
show inventory.....	106
show memory.....	107
show processes cpu.....	108
show processes ipc flow-control.....	109
show processes memory.....	110
show reset-reason.....	112
show revision.....	113
show server-interfaces.....	114
show system.....	115
show tech-support.....	116
show uplink brief.....	120
show util-threshold cpu.....	121
show util-threshold memory.....	121
ssh-peer-stack-unit.....	121
telnet.....	122
telnet-peer-stack-unit.....	122
terminal length.....	123
terminal monitor.....	123
terminal xml.....	123
trace route.....	124
undebg all.....	124
virtual-ip.....	125
write.....	125
<b>Chapter 6: 802.1X.....</b>	<b>127</b>
debug dot1x.....	128
dot1x authentication (Configuration).....	128
dot1x authentication (Interface).....	128
dot1x auth-fail-vlan.....	129
dot1x auth-server.....	129
dot1x auth-type mab-only.....	130
dot1x guest-vlan.....	130
dot1x host-mode.....	131
dot1x mac-auth-bypass.....	131

dot1x max-eap-req.....	132
dot1x max-suplicants.....	132
dot1x port-control.....	132
dot1x quiet-period.....	133
dot1x reauthentication.....	133
dot1x reauth-max.....	134
dot1x server-timeout.....	134
dot1x supplicant-timeout.....	135
dot1x tx-period.....	135
show dot1x cos-mapping interface.....	135
show dot1x interface.....	136

**Chapter 7: Access Control Lists (ACL)..... 139**

Commands Common to all ACL Types.....	141
description.....	141
remark.....	141
resequence access-list.....	142
resequence prefix-list ipv4.....	143
show config.....	144
Common IP ACL Commands.....	144
access-class.....	144
clear counters ip access-group.....	145
ip access-group.....	145
show ip access-lists.....	146
show ip accounting access-list.....	146
Standard IP ACL Commands.....	147
ip access-list standard.....	147
permit (for Standard IP ACLs).....	148
seq.....	149
Extended IP ACL Commands.....	151
deny (for Extended IP ACLs).....	151
deny icmp.....	152
deny tcp.....	154
deny udp.....	156
ip access-list extended.....	158
permit (for Extended IP ACLs).....	158
permit icmp.....	160
permit tcp.....	161
permit udp.....	163
seq.....	165
Common MAC Access List Commands.....	167
clear counters mac access-group.....	168
mac access-group.....	168
show mac access-lists.....	169
show mac accounting access-list.....	169
Standard MAC ACL Commands.....	170
deny.....	170
deny.....	171
mac access-list extended.....	172
permit.....	173

seq.....	174
Extended MAC ACL Commands.....	175
mac access-list standard.....	176
permit.....	176
seq.....	177
IP Prefix List Commands.....	178
clear ip prefix-list.....	178
deny.....	179
ip prefix-list.....	179
permit.....	180
seq.....	180
show config.....	181
show ip prefix-list detail.....	181
show ip prefix-list summary.....	182
Route Map Commands.....	182
continue.....	182
description.....	183
match interface.....	183
match ip address.....	184
match ip next-hop.....	184
match ip route-source.....	185
match metric.....	185
match route-type.....	186
match tag.....	187
route-map.....	187
set automatic-tag.....	188
set metric.....	188
set metric-type.....	189
set tag.....	189
show config.....	189
show route-map.....	190
deny (for Standard IP ACLs).....	190
deny.....	192
seq.....	193
deny tcp.....	195
deny udp.....	197
deny arp (for Extended MAC ACLs).....	199
deny icmp.....	200
deny ether-type (for Extended MAC ACLs).....	202
deny.....	203
deny.....	204
permit (for Standard IP ACLs).....	206
permit.....	207
permit ether-type (for Extended MAC ACLs).....	209
permit icmp.....	210
permit udp.....	212
permit (for Extended IP ACLs).....	214
permit.....	215
seq.....	216
permit tcp.....	218

seq arp.....	220
seq ether-type.....	222
seq.....	224
seq.....	226
permit udp.....	228
permit tcp.....	230
permit icmp.....	232
permit.....	233
deny udp (for IPv6 ACLs).....	234
deny tcp (for IPv6 ACLs).....	236
deny icmp (for Extended IPv6 ACLs).....	238
deny (for IPv6 ACLs).....	239

**Chapter 8: Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM)... 241**

member vlan.....	241
ip access-group.....	242
show acl-vlan-group .....	242
show cam-acl-vlan.....	243
cam-acl-vlan.....	244
show cam-usage.....	245
show running config acl-vlan-group.....	246
acl-vlan-group.....	247
show acl-vlan-group detail.....	247
description (ACL VLAN Group).....	248

**Chapter 9: Bidirectional Forwarding Detection (BFD)..... 249**

bfd all-neighbors.....	249
bfd disable.....	251
bfd enable (Configuration).....	251
bfd enable (Interface).....	251
bfd interval .....	252
bfd protocol-liveness.....	252
ip route bfd.....	253
ip ospf bfd all-neighbors.....	254
ipv6 ospf bfd all-neighbors.....	255
isis bfd all-neighbors.....	255
neighbor bfd.....	256
neighbor bfd disable.....	257
show bfd neighbors.....	257
vrrp bfd neighbor.....	258

**Chapter 10: Border Gateway Protocol IPv4 (BGPv4)..... 260**

BGPv4 Commands.....	262
address-family.....	262
aggregate-address.....	263
bgp add-path.....	263
bgp always-compare-med.....	264
bgp asnotation.....	264
bgp bestpath as-path ignore.....	265

bgp bestpath as-path multipath-relax.....	266
bgp bestpath med confed.....	266
bgp bestpath med missing-as-best.....	266
bgp bestpath router-id ignore.....	267
bgp client-to-client reflection.....	267
bgp cluster-id.....	268
bgp confederation identifier.....	268
bgp confederation peers.....	269
bgp dampening.....	269
bgp default local-preference.....	270
bgp enforce-first-as.....	271
bgp fast-external-failover.....	271
bgp four-octet-as-support.....	272
bgp graceful-restart.....	272
bgp non-deterministic-med.....	273
bgp outbound-optimization.....	273
bgp recursive-bgp-next-hop.....	274
bgp regex-eval-optz-disable.....	274
bgp router-id.....	275
bgp soft-reconfig-backup.....	275
capture bgp-pdu neighbor.....	276
capture bgp-pdu max-buffer-size.....	276
clear ip bgp.....	277
clear ip bgp dampening.....	277
clear ip bgp flap-statistics.....	278
clear ip bgp peer-group.....	278
debug ip bgp.....	279
debug ip bgp dampening.....	279
debug ip bgp events.....	280
debug ip bgp keepalives.....	280
debug ip bgp notifications.....	281
debug ip bgp soft-reconfiguration.....	281
debug ip bgp updates.....	282
default-metric.....	282
description.....	283
max-paths.....	283
neighbor activate.....	284
neighbor add-path.....	284
neighbor advertisement-interval.....	285
neighbor advertisement-start.....	285
neighbor allowas-in.....	286
neighbor default-originate.....	286
neighbor description.....	287
neighbor distribute-list.....	287
neighbor ebgp-multihop.....	288
neighbor fall-over.....	288
neighbor local-as.....	289
neighbor maximum-prefix.....	289
neighbor password.....	290
neighbor peer-group (assigning peers).....	291

neighbor peer-group (creating group).....	291
neighbor peer-group passive.....	292
neighbor remote-as.....	292
neighbor remove-private-as.....	293
neighbor route-map.....	294
neighbor route-reflector-client.....	294
neighbor shutdown.....	295
neighbor soft-reconfiguration inbound.....	295
neighbor timers.....	296
neighbor timers extended.....	297
neighbor update-source.....	297
neighbor weight.....	298
network.....	298
network backdoor.....	299
redistribute.....	300
redistribute ospf.....	300
router bgp.....	301
shutdown all.....	302
shutdown address-family-ipv4-multicast.....	302
shutdown address-family-ipv4-unicast.....	302
shutdown address-family-ipv6-unicast.....	303
show capture bgp-pdu neighbor.....	303
show config.....	304
show ip bgp.....	304
show ip bgp cluster-list.....	307
show ip bgp community.....	308
show ip bgp community-list.....	310
show ip bgp dampened-paths.....	311
show ip bgp detail.....	311
show ip bgp extcommunity-list.....	313
show ip bgp filter-list.....	313
show ip bgp flap-statistics.....	314
show ip bgp inconsistent-as.....	315
show ip bgp neighbors.....	316
show ip bgp next-hop.....	320
show ip bgp paths.....	320
show ip bgp paths as-path.....	322
show ip bgp paths community.....	322
show ip bgp peer-group.....	323
show ip bgp regexp.....	325
show ip bgp summary.....	326
show running-config bgp.....	328
timers bgp.....	328
timers bgp extended.....	329
MBGP Commands.....	329
debug ip bgp dampening.....	329
distance bgp.....	330
show ip bgp dampened-paths.....	330
BGP Extended Communities (RFC 4360).....	331
set extcommunity rt.....	331

set extcommunity soo.....	332
show ip bgp paths extcommunity.....	332
show ip bgp extcommunity-list.....	333
IPv6 BGP Commands.....	333
bgp soft-reconfig-backup.....	334
clear ip bgp ipv6 unicast soft.....	334
debug ip bgp ipv6 unicast soft-reconfiguration.....	335
ipv6 prefix-list.....	335
show ipv6 prefix-list.....	336
IPv6 MBGP Commands.....	336
show ipv6 mbgproutes.....	336
<b>Chapter 11: Configuration Cloning.....</b>	<b>337</b>
clone-config apply.....	337
clone-config check.....	337
clone-config create.....	338
<b>Chapter 12: Content Addressable Memory (CAM).....</b>	<b>339</b>
CAM Profile Commands.....	339
cam-acl (Configuration).....	339
cam-optimization.....	341
cam-threshold.....	342
show cam-acl.....	342
show cam-acl-egress.....	344
<b>Chapter 13: Control Plane Policing (CoPP).....</b>	<b>345</b>
control-plane-cpuqos.....	345
service-policy rate-limit-cpu-queues.....	345
service-policy rate-limit-protocols.....	346
show cpu-queue rate cp.....	346
show ip protocol-queue-mapping.....	347
show ipv6 protocol-queue-mapping.....	347
show mac protocol-queue-mapping.....	348
<b>Chapter 14: u-Boot.....</b>	<b>349</b>
boot change.....	349
boot show net config retries.....	350
boot write net config retries.....	350
boot zero.....	350
default gateway.....	351
enable.....	351
help.....	351
ignore enable password.....	352
ignore startup-config.....	352
interface management ethernet ip address.....	352
no default gateway.....	353
no interface management ethernet ip address.....	353
reload.....	353
show boot blc.....	354

show boot selection.....	354
show bootflash.....	354
show bootvar.....	355
show default gateway.....	356
show interface management ethernet.....	356
show interface management port config.....	356
syntax help.....	357

**Chapter 15: Data Center Bridging (DCB)..... 358**

advertise dcbx-appln-tlv.....	359
advertise dcbx-tlv.....	360
bandwidth-percentage.....	360
dcb-enable.....	361
dcb-policy buffer-threshold (Global Configuration).....	361
dcb-policy buffer-threshold (Interface Configuration).....	362
clear dcbx counters.....	362
clear ets counters.....	363
clear pfc counters.....	363
dcb enable pfc-queues.....	364
dcb enable auto-detect on-next-reload.....	364
dcb-map stack-unit all stack-ports all.....	366
dcbx-port role.....	366
dcbx version.....	367
debug dcbx.....	368
description.....	368
fc-map.....	369
fcoe-map.....	369
fcoe priority-bits.....	370
iscsi priority-bits.....	371
keepalive.....	371
interface vlan (NPIV proxy gateway).....	372
pfc mode on.....	372
pfc no-drop queues.....	373
priority.....	374
priority-group bandwidth pfc.....	375
priority-pgid.....	376
qos-policy-output ets.....	377
qos-policy-buffer.....	377
priority-list.....	378
scheduler.....	379
show dcb.....	380
show interface dcbx detail.....	380
show interface ets.....	383
show interface pfc.....	386
show interface pfc statistics.....	388
show qos priority-groups.....	389
show qos dcb-map.....	389
show stack-unit stack-ports ets details.....	390
dcb pfc-shared-buffer-size.....	391
dcb pfc-total-buffer-size.....	392



dcb-buffer-threshold .....	393
dcb enable pfc-queues.....	393
dcb {ets   pfc} enable.....	394
service-class buffer shared-threshold-weight.....	394
show stack-unit stack-ports pfc details.....	395

**Chapter 16: Dynamic Host Configuration Protocol..... 397**

Commands to Configure the System to be a DHCP Server.....	397
clear ip dhcp.....	397
debug ip dhcp server.....	398
debug ipv6 dhcp .....	398
default-router.....	398
disable.....	399
dns-server.....	399
domain-name.....	399
excluded-address.....	400
hardware-address.....	400
host-address.....	400
ip dhcp server.....	401
lease.....	401
netbios-name-server.....	402
netbios-node-type.....	402
network.....	403
show ip dhcp binding.....	403
show ip dhcp configuration.....	403
show ip dhcp conflict.....	404
show ip dhcp server.....	404
Commands to Configure the System to be a DHCP Client.....	404
ip address dhcp.....	404
Other Commands Supported by the DHCP Client.....	405
clear ip dhcp client statistics.....	405
debug ip dhcp client events.....	405
debug ip dhcp client packets.....	406
release dhcp interface.....	406
renew dhcp interface.....	407
show ip dhcp client statistics.....	407
show ip dhcp lease.....	408
Commands to Configure Secure DHCP.....	408
arp inspection.....	408
arp inspection-limit.....	409
arp inspection-trust.....	409
clear ip dhcp snooping.....	409
clear ipv6 dhcp snooping binding.....	410
ip dhcp relay source-interface.....	410
ipv6 dhcp relay source-interface.....	411
ip dhcp snooping.....	412
ipv6 dhcp snooping.....	412
ip dhcp snooping database.....	412
ipv6 dhcp snooping database write-delay.....	413
ip dhcp snooping binding.....	413

ip dhcp snooping database renew.....	414
ip dhcp snooping trust.....	414
ipv6 dhcp snooping trust.....	414
ip dhcp source-address-validation.....	415
ip dhcp snooping vlan.....	415
ipv6 dhcp snooping vlan.....	416
ip dhcp relay.....	416
show ip dhcp snooping.....	416
show ipv6 DHCP snooping.....	417
ip dhcp snooping verify mac-address.....	417
ipv6 DHCP snooping verify mac-address.....	418
<b>Chapter 17: Equal Cost Multi-Path (ECMP).....</b>	<b>419</b>
ecmp-group.....	419
hash-algorithm.....	419
hash-algorithm ecmp.....	422
hash-algorithm seed.....	423
ip ecmp-group.....	424
link-bundle-distribution trigger-threshold.....	424
link-bundle-monitor enable.....	424
show config.....	425
show link-bundle distribution.....	425
<b>Chapter 18: FC FLEXIO FPORT.....</b>	<b>426</b>
feature fc.....	427
fc zone.....	427
fc alias.....	428
fc zoneset.....	428
fcoe-map.....	429
fabric.....	430
active-zoneset .....	430
stack-unit port-group port portmode.....	431
show fc ns.....	431
show fc switch.....	433
show fc zoneset.....	433
show fc zone.....	434
show fc alias.....	435
show fcoe-map.....	435
show system stack-unit port-group portmode.....	436
<b>Chapter 19: FIPS Cryptography.....</b>	<b>438</b>
fips mode enable.....	438
show fips status.....	438
show ip ssh.....	439
ssh.....	439
<b>Chapter 20: FIP Snooping.....</b>	<b>442</b>
clear fip-snooping database interface vlan.....	442
clear fip-snooping statistics.....	443

feature fip-snooping.....	443
fip-snooping enable.....	443
fip-snooping fc-map.....	444
fip-snooping port-mode fcf.....	444
show fip-snooping statistics.....	445
debug fip-snooping.....	447
show fip-snooping config.....	448
show fip-snooping enode.....	448
show fip-snooping fcf.....	449
show fip-snooping sessions.....	450
show fip-snooping statistics.....	451
show fip-snooping system.....	453
show fip-snooping vlan.....	454
<b>Chapter 21: Force10 Resilient Ring Protocol (FRRP).....</b>	<b>455</b>
clear frrp.....	455
debug frrp.....	456
description.....	456
disable.....	457
interface.....	457
member-vlan.....	458
mode.....	458
protocol frrp.....	459
show frrp.....	459
timer.....	460
<b>Chapter 22: GARP VLAN Registration (GVRP).....</b>	<b>461</b>
clear gvrp statistics.....	462
debug gvrp.....	462
disable.....	463
garp timers.....	463
gvrp enable.....	464
gvrp registration.....	464
protocol gvrp.....	465
show config.....	465
show garp timers.....	465
show gvrp.....	466
clear gvrp statistics.....	467
show vlan.....	468
<b>Chapter 23: Internet Group Management Protocol (IGMP).....</b>	<b>469</b>
IGMP Commands.....	469
IGMP Snooping Commands.....	470
clear ip igmp groups.....	470
debug ip igmp.....	471
ip igmp access-group.....	471
ip igmp group-join-limit.....	471
ip igmp querier-timeout.....	472
ip igmp query-interval.....	472

ip igmp query-max-resp-time.....	473
ip igmp snooping enable.....	473
ip igmp snooping fast-leave.....	474
ip igmp snooping flood.....	474
ip igmp snooping last-member-query-interval.....	474
ip igmp snooping mrouter.....	475
ip igmp snooping querier.....	475
ip igmp version.....	476
show ip igmp groups.....	476
show ip igmp interface.....	477
show ip igmp snooping mrouter.....	478

**Chapter 24: Interfaces.....479**

Basic Interface Commands.....	479
clear counters.....	479
clear dampening.....	480
cx4-cable-length.....	480
dampening.....	481
description.....	482
errdisable recovery cause.....	483
errdisable recovery interval.....	483
flowcontrol.....	484
interface.....	486
interface loopback.....	487
interface ManagementEthernet.....	487
interface null.....	488
interface range.....	488
interface range macro (define).....	490
interface range macro name.....	491
interface vlan.....	491
intf-type cr4 autoneg.....	492
keepalive.....	492
load-balance.....	493
load-balance hg.....	494
monitor interface.....	495
mtu.....	496
negotiation auto.....	497
portmode hybrid.....	498
rate-interval.....	500
rate-interval (Configuration Mode).....	500
remote-fault-signaling rx.....	501
show config.....	501
show config (from INTERFACE RANGE mode).....	502
show interfaces.....	502
show interfaces configured.....	504
show interfaces dampening.....	505
show interfaces description.....	506
show interfaces stack-unit.....	507
show interfaces status.....	507
show interfaces switchport.....	508

show interfaces transceiver.....	510
show range.....	514
shutdown.....	514
speed (for 1000/10000/auto interfaces).....	515
stack-unit portmode.....	516
wavelength.....	516
Port Channel Commands.....	517
channel-member.....	517
group.....	518
interface port-channel.....	519
minimum-links.....	519
port-channel failover-group.....	520
show config.....	520
show interfaces port-channel.....	521
Time Domain Reflectometer (TDR) Commands.....	523
tdr-cable-test.....	523
show tdr.....	524
Enhanced Validation of Interface Ranges.....	524
UDP Broadcast.....	525
debug ip udp-helper.....	525
ip udp-broadcast-address.....	525
ip udp-helper udp-port.....	526
show ip udp-helper.....	527
Port Interface Commands.....	527
Virtual LAN (VLAN) Commands.....	527
auto vlan.....	528
clear mac-address-table dynamic.....	528
default vlan-id.....	529
feature fc.....	529
monitor interface.....	529
name.....	531
show config (INTERFACE mode).....	531
show config (from INTERFACE VLAN mode).....	532
show config (from PROTOCOL LLDP mode).....	532
show vlan.....	533
speed (for 1000/10000 interfaces).....	534
stack-unit port-group port mode ethernet.....	535
vlan tagged (CMC).....	535
vlan untagged (CMC).....	536
<b>Chapter 25: IPv4 Routing.....</b>	<b>538</b>
arp.....	539
arp learn-enable.....	540
arp retries.....	540
arp timeout.....	540
clear arp-cache.....	541
clear host.....	541
clear ip fib stack-unit.....	542
clear ip route.....	542
clear tcp statistics.....	543

debug arp.....	543
debug ip dhcp.....	543
debug ip icmp.....	544
debug ip packet.....	545
icmp6-redirect enable.....	547
ip address.....	547
ip directed-broadcast.....	548
ip domain-list.....	548
ip domain-lookup.....	549
ip domain-name.....	549
ip helper-address.....	550
ip helper-address hop-count disable.....	550
ip host.....	551
ip icmp source-interface.....	551
ipv6 icmp source-interface.....	552
ip max-frag-count.....	553
ip name-server.....	553
ip proxy-arp.....	554
ip route.....	554
ip source-route.....	555
ip tcp initial-time.....	555
show ip tcp initial-time.....	556
ip unreachable.....	556
management route.....	556
show arp.....	557
show arp retries.....	558
show hosts.....	558
show ip cam stack-unit.....	559
show ip fib stack-unit.....	561
show ip interface.....	562
show ip management-route.....	564
show ip multicast-cam stack-unit.....	564
show ip protocols.....	565
show ip route.....	566
show ip route list.....	567
show ip route summary.....	568
show ip traffic.....	569
show tcp statistics.....	570
<b>Chapter 26: Internet Protocol Security (IPSec).....</b>	<b>573</b>
crypto ipsec transform-set.....	573
crypto ipsec policy.....	574
management crypto-policy.....	575
match.....	575
session-key.....	576
show crypto ipsec transform-set.....	576
show crypto ipsec policy.....	577
transform-set.....	578

<b>Chapter 27: IPv6 Access Control Lists (IPv6 ACLs).....</b>	<b>579</b>
IPv6 ACL Commands.....	579
cam-acl.....	579
cam-acl-egress.....	580
ipv6 access-list.....	581
ipv6 control-plane egress-filter.....	581
permit.....	582
permit icmp.....	583
show cam-acl.....	584
show cam-acl-egress.....	585
<b>Chapter 28: IPv6 Basics.....</b>	<b>586</b>
clear ipv6 fib.....	586
clear ipv6 route.....	587
clear ipv6 mld_host.....	587
ipv6 address autoconfig.....	587
ipv6 address.....	588
ipv6 address eui64.....	589
ipv6 control-plane icmp error-rate-limit.....	589
ipv6 flowlabel-zero.....	590
ipv6 host.....	590
ipv6 name-server.....	590
ipv6 nd dad attempts.....	591
ipv6 nd disable-reachable-timer.....	591
ipv6 nd dns-server.....	592
ipv6 nd prefix.....	592
ipv6 nd reachable-time.....	593
ipv6 route.....	593
ipv6 unicast-routing.....	595
show ipv6 cam stack-unit.....	595
show ipv6 control-plane icmp.....	596
show ipv6 fib stack-unit.....	596
show ipv6 flowlabel-zero.....	597
show ipv6 interface.....	597
show ipv6 mld_host.....	599
show ipv6 route.....	600
trust ipv6-diffserv.....	602
<b>Chapter 29: IPv6 Border Gateway Protocol (IPv6 BGP).....</b>	<b>603</b>
IPv6 BGP Commands.....	603
address family.....	603
aggregate-address.....	604
bgp always-compare-med.....	604
bgp bestpath as-path ignore.....	605
bgp bestpath med confed.....	605
bgp bestpath med missing-as-best.....	606
bgp client-to-client reflection.....	606
bgp cluster-id.....	606

bgp confederation identifier.....	607
bgp confederation peers.....	607
bgp dampening.....	608
bgp default local-preference.....	609
bgp enforce-first-as.....	609
bgp fast-external-fallover.....	609
bgp four-octet-as-support.....	610
bgp graceful-restart.....	610
bgp log-neighbor-changes.....	611
bgp non-deterministic-med.....	611
bgp recursive-bgp-next-hop.....	612
bgp regex-eval-optz-disable.....	612
bgp router-id.....	613
bgp soft-reconfig-backup.....	613
capture bgp-pdu neighbor (ipv6).....	614
capture bgp-pdu max-buffer-size.....	614
clear ip bgp * (asterisk).....	614
clear ip bgp as-number.....	615
clear ip bgp ipv6-address.....	616
clear ip bgp peer-group.....	616
clear ip bgp ipv6 dampening.....	617
clear ip bgp ipv6 flap-statistics.....	617
clear ip bgp ipv6 unicast soft.....	618
debug ip bgp.....	618
debug ip bgp events.....	619
debug ip bgp ipv6 dampening.....	620
debug ip bgp ipv6 unicast soft-reconfiguration.....	620
debug ip bgp keepalives.....	621
debug ip bgp notifications.....	621
debug ip bgp updates.....	622
default-metric.....	622
description.....	623
distance bgp.....	623
maximum-paths.....	624
neighbor activate.....	624
neighbor advertisement-interval.....	625
neighbor allowas-in.....	625
neighbor default-originate.....	626
neighbor description.....	626
neighbor distribute-list.....	627
neighbor ebgp-multihop.....	627
neighbor fall-over.....	628
neighbor filter-list.....	628
neighbor maximum-prefix.....	629
neighbor X:X:X::X password.....	630
neighbor next-hop-self.....	630
neighbor peer-group (assigning peers).....	630
neighbor peer-group (creating group).....	631
neighbor peer-group passive.....	632
neighbor remote-as.....	632



neighbor remove-private-as.....	633
neighbor route-map.....	633
neighbor route-reflector-client.....	634
neighbor send-community.....	634
neighbor shutdown.....	635
neighbor soft-reconfiguration inbound.....	635
neighbor subnet.....	636
neighbor timers.....	636
neighbor update-source.....	637
neighbor weight.....	638
network.....	638
network backdoor.....	639
redistribute.....	639
redistribute isis.....	640
redistribute ospf.....	640
router bgp.....	641
show capture bgp-pdu neighbor.....	641
show config.....	642
show ip bgp ipv6 unicast.....	642
show ip bgp ipv6 unicast cluster-list.....	643
show ip bgp ipv6 unicast community.....	643
show ip bgp ipv6 unicast community-list.....	644
show ip bgp ipv6 unicast dampened-paths.....	644
show ip bgp ipv6 unicast detail.....	644
show ip bgp ipv6 unicast extcommunity-list.....	645
show ip bgp ipv6 unicast filter-list.....	645
show ip bgp ipv6 unicast flap-statistics.....	645
show ip bgp ipv6 unicast inconsistent-as.....	646
show ip bgp ipv6 unicast neighbors.....	646
show ip bgp ipv6 unicast peer-group.....	649
show ip bgp ipv6 unicast summary.....	650
show ip bgp next-hop.....	651
show ip bgp paths.....	651
show ip bgp paths as-path.....	652
show ip bgp paths community.....	652
show ip bgp paths extcommunity.....	652
show ip bgp regexp.....	652
timers bgp.....	653
IPv6 MBGP Commands.....	654
address family.....	654
aggregate-address.....	654
bgp dampening.....	655
clear ip bgp ipv6 unicast.....	655
clear ip bgp ipv6 unicast dampening.....	656
clear ip bgp ipv6 unicast flap-statistics.....	656
debug ip bgp ipv6 unicast dampening.....	657
debug ip bgp ipv6 unicast peer-group updates.....	657
debug ip bgp ipv6 unicast updates.....	658
distance bgp.....	658
neighbor activate.....	659

neighbor advertisement-interval.....	659
neighbor default-originate.....	660
neighbor distribute-list.....	660
neighbor filter-list.....	661
neighbor maximum-prefix.....	661
neighbor next-hop-self.....	662
neighbor remove-private-as.....	662
neighbor route-map.....	663
neighbor route-reflector-client.....	663
network.....	664
redistribute.....	664
show ip bgp ipv6 unicast.....	665
show ip bgp ipv6 unicast cluster-list.....	665
show ip bgp ipv6 unicast community.....	666
show ip bgp ipv6 unicast community-list.....	666
show ip bgp ipv6 unicast dampened-paths.....	667
show ip bgp ipv6 unicast detail.....	667
show ip bgp ipv6 unicast filter-list.....	668
show ip bgp ipv6 unicast flap-statistics.....	668
show ip bgp ipv6 unicast inconsistent-as.....	669
show ip bgp ipv6 unicast neighbors.....	669
show ip bgp ipv6 unicast peer-group.....	672
show ip bgp ipv6 unicast summary.....	672
<b>Chapter 30: iSCSI Optimization.....</b>	<b>674</b>
advertise dcbx-app-tlv.....	674
iscsi aging time.....	674
iscsi cos.....	675
iscsi enable.....	676
iscsi priority-bits.....	676
iscsi profile-compellent.....	677
iscsi target port.....	677
show iscsi.....	678
show iscsi sessions.....	678
show iscsi sessions detailed.....	679
show run iscsi.....	679
<b>Chapter 31: Intermediate System to Intermediate System (IS-IS).....</b>	<b>681</b>
adjacency-check.....	682
advertise.....	683
area-password.....	683
clear config.....	684
clear isis.....	684
clns host.....	684
debug isis.....	685
debug isis adj-packets.....	685
debug isis local-updates.....	686
debug isis snp-packets.....	686
debug isis spf-triggers.....	686

debug isis update-packets.....	687
default-information originate.....	687
description.....	688
distance.....	688
distribute-list in.....	689
distribute-list out.....	689
distribute-list redistributed-override.....	690
domain-password.....	690
graceful-restart ietf.....	691
graceful-restart interval.....	691
graceful-restart t1.....	692
graceful-restart t2.....	692
graceful-restart t3.....	693
graceful-restart restart-wait.....	693
hello padding.....	694
hostname dynamic.....	694
ignore-lsp-errors.....	695
ip router isis.....	695
ipv6 router isis.....	695
isis circuit-type.....	696
isis csnp-interval.....	697
isis csnp-interval.....	697
isis hello-multiplier.....	698
isis hello padding.....	698
isis ipv6 metric.....	699
isis metric.....	699
isis network point-to-point.....	700
isis password.....	700
isis priority.....	701
is-type.....	701
log-adjacency-changes.....	702
lsp-gen-interval.....	702
lsp-mtu.....	703
lsp-refresh-interval.....	703
max-area-addresses.....	704
max-lsp-lifetime.....	704
maximum-paths.....	705
metric-style.....	705
multi-topology.....	706
net.....	706
passive-interface.....	707
redistribute.....	707
redistribute bgp.....	708
redistribute ospf.....	709
router isis.....	710
set-overload-bit.....	711
show config.....	711
show isis database.....	712
show isis graceful-restart detail.....	714
show isis hostname.....	714

show isis interface.....	715
show isis neighbors.....	716
show isis protocol.....	717
show isis traffic.....	717
spf-interval.....	719
<b>Chapter 32: Isolated Networks.....</b>	<b>720</b>
io-aggregator isolated-network vlan.....	720
show io-aggregator isolated-networks .....	720
<b>Chapter 33: Link Aggregation Control Protocol (LACP).....</b>	<b>722</b>
auto-lag enable.....	722
clear lacp counters.....	722
debug lacp.....	723
io-aggregator auto-lag enable.....	723
lacp link-fallback.....	724
lacp long-timeout.....	724
lacp port-priority.....	725
port-channel mode.....	725
port-channel-protocol lacp.....	726
show interfaces port-channel.....	727
show io-aggregator auto-lag status.....	729
show lacp.....	729
show link-bundle-distribution port-channel.....	730
show port-channel-flow.....	731
<b>Chapter 34: Layer 2.....</b>	<b>733</b>
MAC Addressing Commands.....	733
clear mac-address-table dynamic.....	733
mac-address-table aging-time.....	734
mac-address-table static.....	734
mac-address-table station-move refresh-arp.....	735
mac learning-limit.....	735
mac learning-limit learn-limit-violation.....	736
mac learning-limit station-move-violation.....	736
mac learning-limit reset.....	737
mac port-security.....	737
show cam mac stack-unit.....	738
show mac-address-table.....	738
show mac-address-table aging-time.....	740
show mac learning-limit.....	741
Virtual LAN (VLAN) Commands.....	741
description.....	742
default vlan-id.....	742
default-vlan disable.....	742
name.....	743
show config.....	743
show vlan.....	744
tagged.....	746

track ip.....	746
untagged.....	747
<b>Chapter 35: Link Layer Discovery Protocol (LLDP).....</b>	<b>748</b>
advertise dot1-tlv.....	748
advertise dot3-tlv.....	749
advertise interface-port-desc.....	749
advertise management-tlv.....	750
clear lldp counters.....	750
clear lldp neighbors.....	751
debug lldp interface.....	751
disable.....	752
hello.....	752
mode.....	753
multiplier.....	753
protocol lldp (Configuration).....	754
protocol lldp (Interface).....	754
show lldp neighbors.....	755
show lldp statistics.....	755
show running-config lldp.....	756
LLDP-MED Commands.....	756
advertise med guest-voice.....	756
advertise med guest-voice-signaling.....	757
advertise med location-identification.....	757
advertise med power-via-mdi.....	758
advertise med softphone-voice.....	759
advertise med streaming-video.....	759
advertise med video-conferencing.....	760
advertise med voice-signaling.....	760
advertise med voice.....	760
advertise med voice-signaling.....	761
<b>Chapter 36: Microsoft Network Load Balancing.....</b>	<b>762</b>
mac-address-table static (for Multicast MAC Address).....	763
ip vlan-flooding.....	764
<b>Chapter 37: Multicast Source Discovery Protocol (MSDP).....</b>	<b>766</b>
clear ip msdp peer.....	766
clear ip msdp sa-cache.....	766
clear ip msdp statistic.....	767
debug ip msdp.....	767
ip msdp cache-rejected-sa.....	768
ip msdp default-peer.....	768
ip msdp log-adjacency-changes.....	769
ip msdp mesh-group.....	769
ip msdp originator-id.....	770
ip msdp peer.....	770
ip msdp redistribute.....	771
ip msdp sa-filter.....	771

ip msdp sa-limit.....	772
ip msdp shutdown.....	772
ip multicast-msdp.....	773
show ip msdp.....	773
show ip msdp sa-cache rejected-sa.....	774
<b>Chapter 38: Multiple Spanning Tree Protocol (MSTP).....</b>	<b>775</b>
debug spanning-tree mstp.....	775
description.....	776
disable.....	776
disable.....	777
forward-delay.....	777
hello-time.....	777
max-age.....	778
max-hops.....	778
msti.....	779
name.....	779
port-channel path-cost custom.....	780
protocol spanning-tree mstp.....	780
revision.....	781
show config.....	781
show spanning-tree mst configuration.....	782
show spanning-tree msti.....	782
spanning-tree.....	784
spanning-tree msti.....	784
spanning-tree mstp.....	785
tc-flush-standard.....	786
<b>Chapter 39: Multicast.....</b>	<b>787</b>
IPv4 Multicast Commands.....	787
clear ip mroute.....	787
ip mroute.....	788
ip multicast-limit.....	788
ip multicast-routing.....	789
mtrace.....	789
show ip mroute.....	790
show ip rpf.....	792
IPv6 Multicast Commands.....	793
debug ipv6 mld_host.....	793
ip multicast-limit.....	794
<b>Chapter 40: Neighbor Discovery Protocol (NDP).....</b>	<b>795</b>
clear ipv6 neighbors.....	795
ipv6 neighbor.....	796
show ipv6 neighbors.....	796
<b>Chapter 41: NPIV Proxy Gateway.....</b>	<b>798</b>
dcb-map.....	798
description (for FCoE maps).....	799

fabric-id vlan.....	799
fcf-priority.....	800
fc-map.....	801
fcoe-map.....	801
feature fc.....	802
fka-adv-period.....	803
keepalive.....	803
show fcoe-map.....	804
show fc sw.....	805
show interfaces status.....	806
show npiv devices.....	807
show qos dcb-map.....	809
show running-config fcoe-map.....	810
<b>Chapter 42: Open Shortest Path First (OSPFv2 and OSPFv3).....</b>	<b>811</b>
OSPFv2 Commands.....	813
area default-cost.....	813
area nssa.....	813
area range.....	814
area stub.....	815
auto-cost.....	815
clear ip ospf.....	815
clear ip ospf statistics.....	816
debug ip ospf.....	816
default-information originate.....	818
default-metric.....	819
description.....	819
distance.....	819
distance ospf.....	820
distribute-list in.....	820
distribute-list out.....	821
fast-convergence.....	822
flood-2328.....	822
graceful-restart grace-period.....	823
graceful-restart helper-reject.....	823
graceful-restart mode.....	823
graceful-restart role.....	824
ip ospf auth-change-wait-time.....	824
ip ospf authentication-key.....	825
ip ospf cost.....	825
ip ospf dead-interval.....	825
ip ospf hello-interval.....	826
ip ospf message-digest-key.....	826
ip ospf mtu-ignore.....	827
ip ospf network.....	827
ip ospf priority.....	828
ip ospf retransmit-interval.....	828
ip ospf transmit-delay.....	829
log-adjacency-changes.....	829
maximum-paths.....	829

mib-binding.....	830
network area.....	830
passive-interface.....	831
redistribute.....	832
redistribute bgp.....	833
redistribute isis.....	833
router-id.....	834
router ospf.....	834
show config.....	835
show ip ospf.....	835
show ip ospf asbr.....	836
show ip ospf database.....	837
show ip ospf database asbr-summary.....	838
show ip ospf database external.....	839
show ip ospf database network.....	841
show ip ospf database nssa-external.....	843
show ip ospf database opaque-area.....	843
show ip ospf database opaque-as.....	844
show ip ospf database opaque-link.....	845
show ip ospf database router.....	846
show ip ospf database summary.....	848
show ip ospf interface.....	849
show ip ospf neighbor.....	851
show ip ospf routes.....	851
show ip ospf statistics.....	852
show ip ospf timers rate-limit.....	855
show ip ospf topology.....	855
summary-address.....	856
timers spf.....	856
timers throttle lsa all.....	857
timers throttle lsa arrival.....	858
OSPFv3 Commands.....	858
area authentication.....	858
area encryption.....	859
area nssa.....	860
auto-cost.....	861
clear ipv6 ospf process.....	862
debug ipv6 ospf.....	862
debug ipv6 ospf bfd.....	863
debug ipv6 ospf events.....	864
debug ipv6 ospf packet.....	865
debug ipv6 ospf spf.....	866
default-information originate.....	867
graceful-restart grace-period.....	868
graceful-restart mode.....	868
ipv6 ospf area.....	869
ipv6 ospf authentication.....	869
ipv6 ospf bfd all-neighbors.....	870
ipv6 ospf cost.....	871
ipv6 ospf dead-interval.....	871



ipv6 ospf encryption.....	872
ipv6 ospf graceful-restart helper-reject.....	873
ipv6 ospf hello-interval.....	873
ipv6 ospf priority.....	874
ipv6 router ospf.....	874
maximum-paths.....	874
passive-interface.....	875
redistribute.....	875
router-id.....	876
show crypto ipsec policy.....	877
show crypto ipsec sa ipv6.....	878
show ipv6 ospf database.....	878
show ipv6 ospf interface.....	879
show ipv6 ospf neighbor.....	879
snmp context.....	880
timers spf.....	880
<b>Chapter 43: Policy-based Routing (PBR).....</b>	<b>882</b>
description.....	882
ip redirect-group.....	882
ip redirect-list.....	883
permit.....	884
redirect.....	885
seq.....	886
show cam pbr.....	888
show ip redirect-list.....	888
<b>Chapter 44: PIM-Sparse Mode (PIM-SM).....</b>	<b>890</b>
IPv4 PIM-Sparse Mode Commands.....	891
clear ip pim rp-mapping.....	891
clear ip pim tib.....	891
debug ip pim.....	891
ip pim bsr-border.....	892
ip pim bsr-candidate.....	893
ip pim dr-priority.....	893
ip pim join-filter.....	894
ip pim ingress-interface-map.....	894
ip pim neighbor-filter.....	895
ip pim query-interval.....	895
ip pim register-filter.....	895
ip pim rp-address.....	896
ip pim rp-candidate.....	896
ip pim sparse-mode.....	897
ip pim sparse-mode sg-expiry-timer.....	897
ip pim spt-threshold.....	898
no ip pim snooping dr-flood.....	898
show ip pim bsr-router.....	899
show ip pim interface.....	899
show ip pim neighbor.....	900

show ip pim rp.....	901
show ip pim snooping interface.....	902
show ip pim snooping neighbor.....	902
show ip pim snooping tib.....	903
show ip pim summary.....	905
show ip pim tib.....	906
show running-config pim.....	907
IPv6 PIM-Sparse Mode Commands.....	907
ipv6 pim bsr-border.....	908
ipv6 pim bsr-candidate.....	908
ipv6 pim dr-priority.....	908
ipv6 pim join-filter.....	909
ipv6 pim query-interval.....	909
ipv6 pim neighbor-filter.....	910
ipv6 pim register-filter.....	910
ipv6 pim rp-address.....	911
ipv6 pim rp-candidate.....	911
ipv6 pim sparse-mode.....	912
ipv6 pim spt-threshold.....	912
show ipv6 pim bsr-router.....	913
show ipv6 pim interface.....	913
show ipv6 pim neighbor.....	914
show ipv6 pim rp.....	914
show ipv6 pim tib.....	915
<b>Chapter 45: Port Monitoring.....</b>	<b>916</b>
description.....	916
erpm.....	917
flow-based enable.....	917
rate-limit.....	918
monitor session.....	918
show config.....	919
show monitor session.....	920
show running-config monitor session.....	920
source (port monitoring).....	921
<b>Chapter 46: Private VLAN (PVLAN).....</b>	<b>922</b>
ip local-proxy-arp.....	923
private-vlan mapping secondary-vlan.....	923
private-vlan mode.....	924
show interfaces private-vlan.....	925
show vlan private-vlan.....	926
show vlan private-vlan mapping.....	927
switchport mode private-vlan.....	928
<b>Chapter 47: Per-VLAN Spanning Tree Plus (PVST+).....</b>	<b>930</b>
description.....	930
disable.....	930
edge-port bpdufilter default.....	931

extend system-id.....	931
protocol spanning-tree pvst.....	932
show spanning-tree pvst.....	933
spanning-tree pvst.....	935
spanning-tree pvst err-disable.....	936
tc-flush-standard.....	937
vlan bridge-priority.....	937
vlan forward-delay.....	937
vlan hello-time.....	938
vlan max-age.....	939

**Chapter 48: Quality of Service (QoS)..... 940**

Global Configuration Commands.....	940
qos-rate-adjust.....	940
service-class dot1p-mapping.....	940
Per-Port QoS Commands.....	941
dot1p-priority.....	941
rate police.....	942
rate-shape.....	943
service-class dynamic dot1p.....	943
service-class bandwidth-percentage.....	944
strict-priority unicast.....	945
Policy-Based QoS Commands.....	945
bandwidth-percentage.....	945
class-map.....	946
clear qos statistics.....	947
crypto key zeroize rsa.....	947
ip ssh rekey .....	948
match ip access-group.....	948
match ip vlan.....	949
match ip vrf.....	949
description.....	950
match ip dscp.....	950
match ip precedence.....	951
match mac access-group.....	952
match mac dot1p.....	952
match mac vlan.....	952
policy-aggregate.....	953
policy-map-input.....	953
policy-map-output.....	954
qos-policy-input.....	955
qos-policy-output.....	955
rate police.....	956
rate shape.....	956
service-policy input.....	957
service-policy output.....	957
service-queue.....	958
set.....	959
show qos class-map.....	959
show qos dcb-map.....	959

show qos policy-map.....	960
show qos policy-map-input.....	961
show qos qos-policy-output.....	962
show qos qos-policy-input.....	962
show qos qos-policy-output.....	963
show qos statistics.....	963
show qos wred-profile.....	964
test cam-usage.....	965
trust.....	966
wred.....	967
wred ecn.....	967
wred-profile.....	968
dscp.....	969
qos dscp-color-map.....	970
qos dscp-color-policy.....	970
show qos dscp-color-policy.....	971
show qos dscp-color-map.....	971
show qos dot1p-queue-mapping.....	972
trust.....	972

**Chapter 49: Routing Information Protocol (RIP).....974**

auto-summary.....	974
clear ip rip.....	975
debug ip rip.....	975
default-information originate.....	976
default-metric.....	976
description.....	977
distance.....	977
distribute-list in.....	977
distribute-list out.....	978
ip poison-reverse.....	979
ip rip receive version.....	979
ip rip send version.....	979
ip split-horizon.....	980
maximum-paths.....	980
neighbor.....	981
network.....	981
offset-list.....	982
output-delay.....	982
passive-interface.....	983
redistribute.....	983
redistribute ospf.....	984
router rip.....	984
show config.....	985
show ip rip database.....	985
show running-config rip.....	986
timers basic.....	987
version.....	987

<b>Chapter 50: Remote Monitoring (RMON)</b> .....	<b>989</b>
rmon alarm.....	989
rmon collection history.....	990
rmon collection statistics.....	991
rmon event.....	991
rmon hc-alarm.....	992
show rmon.....	992
show rmon alarms.....	993
show rmon events.....	994
show rmon hc-alarm.....	995
show rmon history.....	996
show rmon log.....	996
show rmon statistics.....	997
<b>Chapter 51: Rapid Spanning Tree Protocol (RSTP)</b> .....	<b>999</b>
bridge-priority.....	999
debug spanning-tree rstp.....	999
description.....	1000
disable.....	1000
forward-delay.....	1001
hello-time.....	1001
max-age.....	1002
edge-port bpdufilter default.....	1002
protocol spanning-tree rstp.....	1003
show config.....	1003
spanning-tree rstp.....	1004
spanning-tree rstp.....	1005
tc-flush-standard.....	1006
<b>Chapter 52: Security</b> .....	<b>1007</b>
AAA Accounting Commands.....	1007
aaa accounting.....	1007
aaa accounting suppress.....	1008
aaa authorization commands.....	1009
aaa authorization config-commands.....	1009
aaa authorization exec.....	1010
accounting.....	1010
crypto key zeroize rsa.....	1011
show accounting.....	1011
Authentication and Password Commands.....	1012
aaa authentication enable.....	1012
aaa authentication login.....	1013
authorization.....	1014
aaa authorization commands.....	1014
<b>aaa authorization role-only</b> .....	1015
aaa authorization config-commands.....	1016
aaa authorization exec.....	1016
aaa reauthenticate enable.....	1017

privilege level (CONFIGURATION mode).....	1017
privilege level (LINE mode).....	1018
banner exec.....	1018
banner login.....	1019
banner motd.....	1020
debug radius.....	1021
debug tacacs+.....	1021
exec-banner.....	1022
access-class.....	1022
enable password.....	1022
enable restricted.....	1023
enable secret.....	1024
enable sha256-password.....	1024
login authentication.....	1025
password.....	1026
password-attributes.....	1026
service password-encryption.....	1027
show privilege.....	1028
show users.....	1028
secure-cli enable.....	1029
timeout login response.....	1029
username.....	1030
RADIUS Commands.....	1031
client.....	1031
client-key.....	1032
coa-bounce-port.....	1032
coa-disable-port.....	1033
coa-reauthenticate.....	1033
debug radius.....	1033
da-rsp-timeout.....	1034
disconnect-user.....	1034
dynamic-auth-enable.....	1035
ip radius source-interface.....	1035
port.....	1036
radius dynamic-auth.....	1036
radius-server deadtime.....	1036
radius-server host.....	1037
radius-server key.....	1038
radius-server retransmit.....	1038
radius-server timeout.....	1039
<b>role</b> .....	1039
rate-limit.....	1040
replay-protection-window.....	1041
terminate-session.....	1041
show privilege.....	1041
Suppressing AAA Accounting for Null Username Sessions.....	1042
TACACS+ Commands.....	1042
TACACS+ Accounting.....	1042
debug tacacs+.....	1043
ip tacacs source-interface.....	1043

tacacs-server host.....	1044
tacacs-server key.....	1045
timeout login response.....	1045
SSH Server and SCP Commands.....	1046
crypto key generate.....	1046
debug ip ssh.....	1046
ip scp topdir.....	1047
ip ssh authentication-retries.....	1047
ip ssh cipher.....	1048
ip ssh connection-rate-limit.....	1048
ip ssh hostbased-authentication.....	1049
ip ssh key-size.....	1049
ip ssh mac.....	1050
ip ssh password-authentication.....	1051
ip ssh rhostsfile.....	1051
ip ssh rekey .....	1052
ip ssh rsa-authentication (Config).....	1052
ip ssh rsa-authentication (EXEC).....	1053
ip ssh server.....	1053
ip ssh server dns enable.....	1055
show crypto.....	1055
show ip ssh.....	1056
show ip ssh client-pub-keys.....	1057
show ip ssh rsa-authentication.....	1057
show role.....	1058
show userroles.....	1059
ssh.....	1059
ip ssh pub-key-file.....	1060
Secure DHCP Commands.....	1060
clear ip dhcp snooping.....	1060
ip dhcp relay.....	1061
ip dhcp snooping.....	1061
ip dhcp snooping database.....	1061
ip dhcp snooping binding.....	1062
ip dhcp snooping database renew.....	1062
ip dhcp snooping trust.....	1063
ip dhcp source-address-validation.....	1063
ip dhcp snooping vlan.....	1063
show ip dhcp snooping.....	1064
username.....	1064
<b>userrole</b> .....	1065
ICMP Vulnerabilities.....	1066
drop icmp.....	1067
System Security Commands.....	1067
generate hash.....	1068
root-access password.....	1068
verified boot.....	1069
verified boot hash.....	1069
verified startup-config.....	1070

<b>Chapter 53: sFlow.....</b>	<b>1071</b>
sflow collector.....	1071
sflow enable (Global).....	1072
sflow ingress-enable.....	1073
sflow extended-switch enable.....	1073
sflow max-header-size extended.....	1074
sflow polling-interval (Global).....	1074
sflow polling-interval (Interface).....	1075
sflow sample-rate (Global).....	1075
sflow sample-rate (Interface).....	1076
show sflow.....	1076
show sflow stack-unit.....	1077
<b>Chapter 54: Service Provider Bridging.....</b>	<b>1078</b>
debug protocol-tunnel.....	1078
protocol-tunnel.....	1079
protocol-tunnel destination-mac.....	1079
protocol-tunnel enable.....	1080
protocol-tunnel rate-limit.....	1080
show protocol-tunnel.....	1081
<b>Chapter 55: Simple Network Management Protocol (SNMP) and Syslog.....</b>	<b>1082</b>
SNMP Commands.....	1083
clear logging auditlog.....	1083
show snmp.....	1084
show snmp engineID.....	1084
show snmp group.....	1085
show snmp supported-mibs.....	1085
show snmp supported-traps.....	1086
show snmp user.....	1087
snmp context.....	1087
snmp context.....	1087
snmp ifmib ifalias long.....	1088
snmp-server community.....	1089
snmp-server contact.....	1090
snmp-server enable traps.....	1090
snmp-server engineID.....	1091
snmp-server group.....	1092
snmp-server host.....	1093
snmp-server location.....	1095
snmp-server packetsize.....	1095
snmp-server trap-source.....	1095
snmp-server user.....	1096
snmp-server user (for AES128-CFB Encryption).....	1098
snmp-server view.....	1099
snmp trap link-status.....	1099
Syslog Commands.....	1100
clear logging.....	1100



default logging buffered.....	1100
default logging console.....	1100
logging extended.....	1101
default logging monitor.....	1101
default logging trap.....	1102
logging.....	1102
logging buffered.....	1103
logging console.....	1103
logging facility.....	1104
logging history.....	1105
logging history size.....	1105
logging monitor.....	1106
logging on.....	1106
logging source-interface.....	1107
logging synchronous.....	1107
logging trap.....	1108
logging version.....	1108
show logging.....	1109
show logging driverlog stack-unit.....	1110
show logging auditlog.....	1110
terminal monitor.....	1111
<b>Chapter 56: Stacking Commands.....</b>	<b>1112</b>
power-cycle stack-unit.....	1112
redundancy disable-auto-reboot.....	1113
redundancy force-failover stack-unit.....	1113
reset stack-unit.....	1114
show redundancy.....	1114
show system stack-ports.....	1115
show system stack-unit iom-mode.....	1117
show system stack-unit stack-group.....	1117
stack-unit iom-mode.....	1118
stack-unit priority.....	1119
stack-unit provision.....	1119
stack-unit renumber.....	1119
track-stack-ports disable-all-links.....	1120
<b>Chapter 57: Storm Control.....</b>	<b>1122</b>
io-aggregator broadcast storm-control.....	1122
show io-aggregator broadcast storm-control status.....	1123
show storm-control unknown-unicast.....	1123
show storm-control broadcast.....	1124
show storm-control multicast.....	1124
storm-control multicast (Interface).....	1125
storm-control broadcast (Configuration).....	1125
storm-control broadcast (Interface).....	1126
storm-control multicast (Configuration).....	1126
storm-control PFC/LLFC.....	1127
storm-control unknown-unicast (Configuration).....	1127

storm-control unknown-unicast (Interface).....	1127
--	------

**Chapter 58: SupportAssist..... 1129**

eula-consent.....	1129
support-assist.....	1131
support-assist activate.....	1131
support-assist activity.....	1132
SupportAssist Commands.....	1132
activity.....	1132
contact-company.....	1133
contact-person.....	1133
enable.....	1134
server.....	1135
SupportAssist Activity Commands.....	1135
action-manifest get.....	1135
action-manifest install.....	1136
action-manifest remove.....	1137
action-manifest show.....	1137
enable.....	1138
SupportAssist Company Commands.....	1138
address.....	1138
street-address.....	1139
territory.....	1140
SupportAssist Person Commands.....	1140
email-address.....	1140
phone.....	1141
preferred-method.....	1142
time-zone.....	1142
SupportAssist Server Commands.....	1143
proxy-ip-address.....	1143
enable.....	1144
url.....	1144
show eula-consent.....	1145
show running-config.....	1146
show support-assist status.....	1147

**Chapter 59: Spanning Tree Protocol (STP)..... 1148**

bridge-priority.....	1148
debug spanning-tree.....	1148
description.....	1149
disable.....	1149
forward-delay.....	1150
hello-time.....	1150
max-age.....	1151
portfast bpdupfilter default.....	1151
protocol spanning-tree.....	1151
show config.....	1152
show spanning-tree 0.....	1152
spanning-tree 0.....	1154

<b>Chapter 60: System Time.....</b>	<b>1156</b>
clock set.....	1156
clock summer-time date.....	1157
clock summer-time recurring.....	1158
debug ntp.....	1159
ntp offset-threshold.....	1159
ntp server.....	1160
ntp authenticate.....	1160
ntp authentication-key.....	1160
ntp control-key-passwd.....	1161
ntp master <stratum>.....	1162
ntp server.....	1162
ntp source.....	1163
ntp trusted-key.....	1164
show clock.....	1164
show ntp associations.....	1165
show ntp vrf associations.....	1166
show ntp status.....	1166
<b>Chapter 61: Tunneling .....</b>	<b>1168</b>
tunnel-mode.....	1168
tunnel source.....	1169
tunnel keepalive.....	1169
tunnel allow-remote.....	1170
tunnel dscp.....	1170
tunnel destination.....	1171
tunnel flow-label.....	1171
tunnel hop-limit.....	1172
ip unnumbered.....	1172
ipv6 unnumbered.....	1173
<b>Chapter 62: u-Boot.....</b>	<b>1174</b>
boot change.....	1174
boot selection.....	1175
boot show net config retries.....	1175
boot write net config retries.....	1175
boot zero.....	1176
default gateway.....	1176
enable.....	1176
help.....	1176
ignore enable password.....	1177
ignore startup config.....	1177
interface management ethernet ip address.....	1177
no default-gateway.....	1178
no interface management ethernet ip address.....	1178
reload.....	1178
show boot blc.....	1179
show boot selection.....	1179

show bootflash.....	1179
show bootvar.....	1180
show default-gateway.....	1181
show interface management Ethernet.....	1181
show interface management port config.....	1181
syntax help.....	1182
<b>Chapter 63: Uplink Failure Detection (UFD).....</b>	<b>1183</b>
clear ufd-disable.....	1183
debug uplink-state-group.....	1184
defer-timer.....	1184
description.....	1185
downstream.....	1185
downstream auto-recover.....	1186
downstream disable links.....	1186
enable.....	1187
show running-config uplink-state-group.....	1187
show uplink-state-group.....	1188
uplink-state-group.....	1189
upstream.....	1189
<b>Chapter 64: VLAN Stacking.....</b>	<b>1191</b>
dei enable.....	1191
dei honor.....	1192
dei mark.....	1192
member.....	1193
show interface dei-honor.....	1193
show interface dei-mark.....	1194
vlan-stack access.....	1194
vlan-stack compatible.....	1195
vlan-stack dot1p-mapping.....	1195
vlan-stack protocol-type.....	1196
vlan-stack trunk.....	1196
<b>Chapter 65: Virtual Link Trunking (VLT).....</b>	<b>1199</b>
back-up destination.....	1200
clear ip mroute.....	1200
clear ip pim tib.....	1200
clear vlt statistics.....	1201
delay-restore abort-threshold.....	1201
lACP ungroup member-independent.....	1202
multicast peer-routing timeout.....	1203
peer-link port-channel.....	1203
peer-routing.....	1203
peer-routing-timeout.....	1204
primary-priority.....	1204
show ip mroute.....	1205
show vlt backup-link.....	1206
show vlt brief.....	1207

show vlt detail.....	1207
show vlt inconsistency.....	1208
show vlt mismatch.....	1208
show vlt role.....	1209
show vlt statistics.....	1209
stack-unit iom-mode.....	1211
system-mac.....	1211
unit-id.....	1212
vlt domain.....	1212
vlt-peer-lag port-channel.....	1213
show vlt private-vlan.....	1213
<b>Chapter 66: Virtual Router Redundancy Protocol (VRRP).....</b>	<b>1214</b>
advertise-interval.....	1214
authentication-type.....	1215
clear counters vrrp.....	1215
debug vrrp.....	1216
description.....	1216
disable.....	1217
hold-time.....	1217
preempt.....	1218
priority.....	1218
show config.....	1219
show vrrp.....	1219
track.....	1221
virtual-address.....	1222
vrrp delay minimum.....	1222
vrrp delay reload.....	1223
vrrp-group.....	1223
VRRP for IPv6 Commands.....	1224
clear counters vrrp ipv6.....	1224
debug vrrp ipv6.....	1224
show vrrp ipv6.....	1225
vrrp-ipv6-group.....	1226
version.....	1227
<b>Chapter 67: SNMP Traps.....</b>	<b>1229</b>
<b>Chapter 68: FC Flex IO Modules.....</b>	<b>1233</b>
FC Flex IO Modules.....	1233
Data Center Bridging (DCB) for FC Flex IO Modules.....	1233
NPIV Proxy Gateway for FC Flex IO Modules.....	1233
description (for FCoE maps).....	1233
fabric.....	1234
fabric-id vlan.....	1235
fcf-priority.....	1235
fc-map.....	1236
fcoe-map.....	1236
fka-adv-period.....	1237

interface vlan (NPIV proxy gateway).....	1238
keepalive.....	1239
show fcoe-map.....	1239
show npiv devices.....	1241
<b>Chapter 69: Debugging and Diagnostics.....</b>	<b>1244</b>
Offline Diagnostic Commands.....	1244
Hardware Commands.....	1244
clear hardware stack-unit.....	1245
clear hardware system-flow.....	1245
show hardware layer2 acl.....	1246
show hardware layer3.....	1246
diag stack-unit.....	1246
hardware watchdog.....	1247
online stack-unit.....	1248
offline stack-unit.....	1248
show diag.....	1249
show hardware stack-unit.....	1251
show hardware system-flow.....	1258
show hardware buffer interface.....	1260
show hardware counters interface <i>interface</i> .....	1261
show hardware drops.....	1263
<b>Appendix A: Internet Control Message Protocol (ICMP) Message Types.....</b>	<b>1266</b>

# About this Guide

This book provides information about the Dell Networking OS command line interface (CLI) on the Dell PowerEdge FN I/O Module.

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

## References

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

- *Dell PowerEdge FN I/O Module Configuration Guide*
- *Dell PowerEdge FN I/O Module Getting Started Guide*
- *Release Notes for the Dell System PowerEdge FN I/O Module*


### Topics:

- [Objectives](#)
- [Audience](#)
- [Conventions](#)
- [Information Icons](#)

## Objectives

This book is intended as a reference guide for the FN I/O Module CLI commands, with detailed syntax statements, along with usage information and sample output.

This guide contains an Appendix with a list of the request for comment (RFCs) and management information base files (MIBs) supported.

 **NOTE:** For more information about when to use the CLI commands, refer to the *Dell PowerEdge FN I/O Module 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.


<b>Keyword</b>	Keywords are in Courier font and must be entered in the CLI as listed.
<b><i>parameter</i></b>	Parameters are in italics and require a number or word to be entered in the CLI.
<b>{X}</b>	Keywords and parameters within braces must be entered in the CLI.
<b>[X]</b>	Keywords and parameters within brackets are optional.
<b>x y</b>	Keywords and parameters separated by a bar require you to choose one option.
<b>x  y</b>	Keywords and parameters separated by a double bar allow 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.

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



# Before You Start

By following the instructions in the *Dell PowerEdge FN I/O Module Getting Started Guide* that is shipped with the product, you install the FN I/O Module in a Dell PowerEdge FX2 server chassis.

The Aggregator installs with zero-touch configuration. After you power it on, an Aggregator boots up with default settings and auto-configures with software features enabled. This chapter describes the default settings and software features that are automatically configured at startup. Use the tasks described in the other chapters to reconfigure the Aggregator for customized network operation.

## Topics:

- [Operational Modes](#)
- [Default Settings](#)
- [Other Auto-Configured Settings](#)
- [DCB Support](#)
- [FCoE Connectivity](#)
- [iSCSI Operation](#)
- [Link Aggregation](#)
- [Uplink Failure Detection](#)
- [VLANs](#)
- [Where to Go From Here](#)

## Operational Modes

The FN I/O Module supports four operational modes. Select the operational mode that meets your deployment needs. To enable a new operational mode, reload the switch.

- Standalone mode — `stack-unit unit iom-mode standalone`. This is the default mode for IOA. It is fully automated zero-touch mode that allows you to configure VLAN memberships. (Manageable through CMC also)
- Programmable MUX mode (PMUX) — `stack-unit unit iom-mode programmable-mux`. Select this mode to configure PMUX mode CLI commands.
- Stacking mode — `stack-unit unit iom-mode stacking`. Select this mode to stack up to six IOA stack units as a single logical switch. The stack units can be in the same or on different chassis. This is a low-touch mode where all configuration except VLAN membership is automated. To enable VLAN, you must configure it. In this operational mode, ports 9 and 10 are dedicated to stacking.
- Virtual Link Trunking mode (VLT) — `stack-unit unit iom-mode vlt`. Select this mode to multi-home server interfaces to different IOA modules. This is a low-touch mode where all configuration except VLAN membership is automated. To enable VLAN, you must configure it. In this mode, ports 9 is configured as VLT interconnect.
- Full Switch mode — `stack-unit unit iom-mode full-switch`. The full switch mode provides Layer 2 / Layer 3 functionalities on the Dell FX2 chassis. All the commands and configurations supported on the MXL is available in full-switch mode.

For more information, see the *FN IOM Configuration Guide*.

## Default Settings

The I/O Aggregator provides zero-touch configuration with the following default configuration settings:

- Default user name (**root**)
- Password (**calvin**)
- VLAN (**vlan1**) and IP address for in-band management (**DHCP-assigned**)
- IP address for out-of-band (OOB) management (**DHCP-assigned**)
- Read-only SNMP community name (**public**)

- Broadcast storm control (**enabled**)
- Unregistered Multicast Packets flooding (**enabled**)
- IGMP snooping in all VLANs except the default VLAN (**enabled**)
- VLAN configuration (**all ports belong to all VLANs**)

You can change any of these default settings using the CLI. Refer to the appropriate chapter for details.

**i** **NOTE:** You can also change many of the default settings using the chassis management controller (CMC) interface. For information about how to access the CMC to configure an Aggregator, refer to the *Dell PowerEdge M1000e Enclosure Hardware Owner's Manual* or *Dell Chassis Management Controller (CMC) User's Guide* on the Dell Support website at <http://support.dell.com/support/edocs/systems/pem/en/index.htm>.

## Other Auto-Configured Settings

After the Aggregator powers on, it auto-configures and is operational with software features enabled, including:

- VLANs: All ports are configured as members of all (4094) VLANs. All VLANs are up and can send or receive layer 2 traffic. For more information, refer to [VLANs](#).
- Data Center Bridging Capability Exchange Protocol (DCBX)
- Fibre Channel over Ethernet (FCoE) connectivity
- FCoE Initiation Protocol (FIP) snooping
- Hybrid ports: Ports are administratively up and auto-configured to operate as hybrid ports to transmit tagged and untagged VLAN traffic.
- iSCSI optimization
- IGMP snooping
- Jumbo frames: Ports are set to a maximum MTU of 12,000 bytes by default.
- Link aggregation: All uplink ports are configured in a single LAG (LAG 128).
- Link Layer Discovery Protocol (LLDP): Enabled on all ports.
- Link tracking: Enables server-facing links to be brought up only if the uplink port-channel (LAG 128) is up.

## DCB Support

DCB enhancements for data center networks are supported to eliminate packet loss and provision links with required bandwidth.

The Aggregator provides zero-touch configuration for DCB. The Aggregator auto-configures DCBX port roles to match the DCBX configuration in the ToR switches to which it connects through its uplink ports.

The Aggregator supports DCB only in standalone mode and not in the stacking mode.

## FCoE Connectivity

Many data centers use Fibre Channel (FC) in storage area networks (SANs). Fibre Channel over Ethernet (FCoE) encapsulates Fibre Channel frames over Ethernet networks.

On an Aggregator, the internal ports support FCoE connectivity and connect to the converged network adapter (CNA) in blade servers. FCoE allows Fibre Channel to use 10-Gigabit Ethernet networks while preserving the Fibre Channel protocol.

The Aggregator also provides zero-touch configuration for FCoE configuration. The Aggregator auto-configures to match the FCoE settings used in the ToR switches to which it connects through its uplink ports.

## iSCSI Operation

Support for iSCSI traffic is turned on by default when the Aggregator powers up. No configuration is required.

When the Aggregator powers up, it monitors known TCP ports for iSCSI storage devices on all interfaces. When a session is detected, an entry is created and monitored as long as the session is active.

The Aggregator also detects iSCSI storage devices on all interfaces and auto-configures to optimize performance. Performance optimization operations, such as Jumbo frame size support, and disabling storm control on interfaces connected to an iSCSI equallogic (EQL) storage device, are applied automatically.

CLI configuration is necessary only when the configuration includes iSCSI storage devices that cannot be automatically detected and when non-default QoS handling is required.

## Link Aggregation

In Standalone, Stacking, and VLT modes, all uplink ports (except port 9 in VLT mode) are configured in a single LAG (LAG 128). There can be multiple uplink LAGs in programmable-mux mode. Server-facing ports are auto-configured as part of link aggregation groups if the corresponding server is configured for LACP-based NIC teaming. Static LAGs are supported only in PMUX and Full-Switch modes.

**NOTE:** The default LACP timeout is Long-Timeout. The same timeout is recommended to be configured in peer devices.

## Uplink Failure Detection

By default, all server-facing ports are tracked by the operational status of the uplink LAG. If the uplink LAG goes down, the Aggregator loses its connectivity and is no longer operational; all server-facing ports are brought down.

**NOTE:** If installed servers do not have connectivity to a ToR switch, check the Link Status LED of uplink ports on the Aggregator. If all LEDs are ON, check the LACP configuration on the ToR switch that is connected to the Aggregator to ensure the LACP is correctly configured.

## VLANs

By default, all Aggregator ports belong to all 4094 VLANs and are members of untagged VLAN 1. You can use the CLI or CMC interface to configure only the required VLANs on a port.

When you configure VLANs on server-facing interfaces (ports 1 to 8), you can assign VLANs to a port or a range of ports by entering the `vlan tagged` or `vlan untagged` commands in interface configuration mode; for example:

```
Dell(conf)# interface tengigabitethernet 0/2 - 4
Dell(conf-if-range-te-0/2-4)# vlan tagged 5,7,10-12
Dell(conf-if-range-te-0/2-4)# vlan untagged 3
```

**NOTE:** You can also use the CMC interface to configure VLANs.

### Uplink LAG

The tagged VLAN membership of the uplink LAG is automatically configured based on the tagged and untagged VLAN configuration of all server-facing ports (ports 1 to 8).

The untagged VLAN used for the uplink LAG is always the default VLAN.

### Server-Facing LAGs

The tagged VLAN membership of a server-facing LAG is automatically configured based on the server-facing ports that are members of the LAG.

The untagged VLAN of a server-facing LAG is configured based on the untagged VLAN to which the lowest numbered server-facing port in the LAG belongs.

**NOTE:** Dell Networking recommends that you configure the same VLAN membership on all LAG member ports.

### Stacking Mode

When you configure an Aggregator to operate in stacking mode (See “Configuring and Bringing Up a Stack” in the Dell Networking Configuration Guide for the M I/O Aggregator), VLANs are reconfigured as follows:

If an Aggregator port belonged to all 4094 VLANs in standalone mode (default), all VLAN membership is removed and the port is assigned only to default VLAN 1. You must configure additional VLAN membership as necessary.

If you had manually configured an Aggregator port to belong to one or more VLANs (non-default) in standalone mode, the VLAN configuration is retained in stacking mode only on the master switch.

When you reconfigure an Aggregator from stacking to standalone mode:

Aggregator ports that you manually configured for VLAN membership in stacking mode retain their VLAN configuration in standalone mode.

To restore the default auto-VLAN mode of operation (in which all ports are members of all 4094 VLANs) on a port, enter the `auto vlan` command:

```
Dell(conf)# interface tengigabitethernet 0/2
Dell(conf-if-te-0/2)# auto vlan
```

The `auto vlan` command is applicable only in Standalone mode.

To get the default standalone mode configurations:

- Restore to factory default settings.

## Where to Go From Here

You can customize the Aggregator for use in your data center network as necessary. To perform additional switch configuration, do one of the following:

- For remote out-of-band management, enter the OOB management interface IP address into a Telnet or SSH client and log in to the switch using the user ID and password to access the CLI.
- For local management using the CLI, use the attached console connection.
- For remote in-band management from a network management station, enter the VLAN IP address of the management port and log in to the switch to access the CLI.

If you installed the Aggregator in a stack, you can configure additional settings for switch stacking

In case of a Dell Networking OS upgrade, you can check to see that an Aggregator is running the latest Dell Networking OS version by entering the [show version](#) command. To download a Dell Networking OS version, go to <http://support.dell.com>.

Refer to the appropriate chapter for detailed information on how to configure specific software settings.

# CLI Basics

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

## Topics:

- [Accessing the Command Line](#)
- [Multiple Configuration Users](#)
- [Navigating the CLI](#)
- [Obtaining Help](#)
- [Using the Keyword no Command](#)
- [Filtering show Commands](#)
- [Command Modes](#)
- [Track Login Activity](#)
- [Limit Concurrent Login Sessions](#)

## 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 Modes](#) section.

## Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, the Dell operating system 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, the 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.

## Navigating the CLI

The 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.

**Table 1. CLI Command Modes and Prompts**

Prompt	CLI Command Mode
Dell>	EXEC
Dell#	EXEC Privilege
Dell(conf)#	CONFIGURATION
Dell(conf-if-te-0/1)# Dell(conf-if-vl-1)# Dell(conf-if-ma-0/0)# Dell(conf-if-range)#	INTERFACE
Dell(conf-line-console)# Dell(conf-line-vty)#	LINE
Dell(conf-mon-sess)#	MONITOR SESSION

## 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 ?
igmp      Internet Group Management Protocol
route     Establish static routes
telnet    Specify telnet options
```

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 tengig int` for the `interface tengigabitethernet interface` command.
- To complete keywords in commands, use the TAB key.
- To display the last enabled command, use the up Arrow key.
- To erase the previous character, use either the Backspace key or Delete key.
- 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
<b>CNTL-A</b>	Moves the cursor to the beginning of the command line.
<b>CNTL-B</b>	Moves the cursor back one character.
<b>CNTL-D</b>	Deletes the character at the cursor.
<b>CNTL-E</b>	Moves the cursor to the end of the line.
<b>CNTL-F</b>	Moves the cursor forward one character.
<b>CNTL-I</b>	Completes a keyword.
<b>CNTL-K</b>	Deletes all the characters from the cursor to the end of the command line.
<b>CNTL-L</b>	Re-enters the previous command.
<b>CNTL-N</b>	Returns to the more recent commands in the history buffer after recalling commands with Ctrl-P or the up Arrow key.
<b>CNTL-P</b>	Recalls commands, beginning with the last command.
<b>CNTL-U</b>	Deletes the line.
<b>CNTL-W</b>	Deletes the previous word.
<b>CNTL-X</b>	Deletes the line.
<b>CNTL-Z</b>	Comes back to EXEC mode from any CONFIGURATION mode.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Esc D</b>	Deletes all the characters from the cursor to the end of the word.

## 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. For example:

<b>Syntax</b>	<code>no {boot   default   enable   ftp-server   hardware   hostname   ip   line   logging   monitor   service   io-aggregator broadcast storm-control   snmp-server   username}</code>
<b>Defaults</b>	None

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## 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:** The 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 TenGig|except regular-expression | find regular-expression`.

<b>except</b>	displays only the text that does not match the pattern (or regular expression)
<b>find</b>	searches for the first occurrence of a pattern
<b>grep</b>	displays text that matches a pattern.
<b>no-more</b>	does not paginate the display output
<b>save</b>	copies the output to a file for future use

The `grep` command option has an `ignore-case` sub-option 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 0/1`.
- `show run | grep ethernet` does not return the search result above because it only searches for instances containing a non-capitalized “ethernet”.
- `show run | grep Ethernet ignore-case` returns instances containing both “Ethernet” and “ethernet”.

## Displaying All Output

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

```
Dell#show running-config|no-more
```

## Filtering the Command Output Multiple Times

You can filter a single command output multiple times. To filter a command output multiple times, place the `save` option as the last filter. For example:

```
Dell# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save
```




# Command Modes

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

## 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 displays.

## 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.

## INTERFACE Mode

To configure interfaces or IP services on those interfaces, use INTERFACE mode. An interface can be physical (for example, a TenGigabit Ethernet port) or virtual (for example, the VLAN interface).

To enter INTERFACE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `interface` command and then enter an interface type and interface number that is available on the switch.

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

Prompt	Interface Type
Dell (conf-if-te-0/1) #	Ten-Gigabit Ethernet interface then slot/port information
Dell (conf-if-vl-1) #	VLAN Interface then VLAN number (range 1–4094)
Dell (conf-if-ma-0/0) #	Management Ethernet interface then slot/port information
Dell (conf-if-range) #	Designated interface range (used for bulk configuration)

## 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 `vtty` 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.

## MONITOR SESSION Mode

In CONFIGURATION mode, use the `monitor session` command to enter MONITOR SESSION mode and configure port monitoring.

To enter MONITOR SESSION mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `monitor session` command. Include the monitor session ID. The prompt changes to include `(conf-mon-sess)`.

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

## PROTOCOL LLDP Mode

In CONFIGURATION mode, use the `protocol lldp` command to enter PROTOCOL LLDP mode and configure the LLDP protocol.

To enter PROTOCOL LLDP mode:

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

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

# Track Login Activity

Dell Networking OS enables you to track the login activity of users and view the successful and unsuccessful login events.

When you log in using the console or VTY line, the system displays the last successful login details of the current user and the number of unsuccessful login attempts since your last successful login to the system. The system stores the number of unsuccessful login attempts that have occurred in the last 30 days by default. You can change the default value to any number of days from 1 to 30. By default, login activity tracking is disabled. You can enable it using the `login statistics enable` command from the configuration mode.

## Restrictions for Tracking Login Activity

These restrictions apply for tracking login activity:

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

## Configuring Login Activity Tracking

To enable and configure login activity tracking, follow these steps:

1. Enable login activity tracking.  
CONFIGURATION mode  
`login statistics enable`

After enabling login statistics, the system stores the login activity details for the last 30 days.

- (Optional) Configure the number of days for which the system stores the user login statistics. The range is from 1 to 30.

CONFIGURATION mode

```
login statistics time-period days
```

The following example enables login activity tracking. The system stores the login activity details for the last 30 days.

```
Dell(config)#login statistics enable
```

The following example enables login activity tracking and configures the system to store the login activity details for 12 days.

```
Dell(config)#login statistics enable
Dell(config)#login statistics time-period 12
```

## Display Login Statistics

To view the login statistics, use the `show login statistics` command.

### Example of the `show login statistics` Command

The `show login statistics` command displays the successful and failed login details of the current user in the last 30 days or the custom defined time period.

```
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
-----
```

### Example of the `show login statistics all` command

The `show login statistics all` command displays the successful and failed login details of all users in the last 30 days or the custom defined time period.

```
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
-----
```

### Example of the `show login statistics user user-id` command

The `show login statistics user user-id` command displays the successful and failed login details of a specific user in the last 30 days or the custom defined time period.

```
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
-----
```

## Limit Concurrent Login Sessions

Dell Networking OS enables you to limit the number of concurrent login sessions of users on VTY, Aux, and console lines. You can also clear any of your existing sessions when you reach the maximum permitted number of concurrent sessions.

By default, you can use all 10 VTY lines, one console line, and one Aux line. You can limit the number of available sessions using the `login concurrent-session limit` command and so restrict users to that specific number of sessions. You can optionally configure the system to provide an option to the users to clear any of their existing sessions.

## Restrictions for Limiting the Number of Concurrent Sessions

These restrictions apply for limiting the number of concurrent sessions:

- Only the system and security administrators can limit the number of concurrent sessions and enable the clear-line option.
- Users can clear their existing sessions only if the system is configured with the `login concurrent-session clear-line enable` command.

## Configuring Concurrent Session Limit

To configure concurrent session limit, follow this procedure:

- Limit the number of concurrent sessions for all users.  
CONFIGURATION mode  
`login concurrent-session limit number-of-sessions`

The following example limits the permitted number of concurrent login sessions to 4.

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

## Enabling the System to Clear Existing Sessions

To enable the system to clear existing login sessions, follow this procedure:

- Use the following command.  
CONFIGURATION mode  
`login concurrent-session clear-line enable`

The following example enables you to clear your existing login sessions.

```
Dell(config)#login concurrent-session clear-line enable
```

### Example of Clearing Existing Sessions

When you try to login, 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 the existing sessions. If you close any of the existing sessions, you are allowed to login. :

```
$ telnet 10.11.178.17
Trying 10.11.178.17...
Connected to 10.11.178.17.
Escape character is '^]'.
Login: admin
Password:

Maximum concurrent sessions for the user reached.
Current VTY 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
Kill existing session? [line number/Enter to cancel]:
```

# File Management

This chapter contains commands needed to manage the configuration files and includes other file management commands.

## Topics:

- [boot system gateway](#)
- [boot system stack-unit](#)
- [cd](#)
- [copy](#)
- [copy running-config startup-config](#)
- [delete](#)
- [dir](#)
- [format flash](#)
- [HTTP Copy via CLI](#)
- [logging coredump stack-unit](#)
- [logging coredump server](#)
- [pwd](#)
- [rename](#)
- [restore factory-defaults](#)
- [show boot system](#)
- [show file](#)
- [show file-systems](#)
- [show os-version](#)
- [show running-config](#)
- [show startup-config](#)
- [show version](#)
- [upgrade boot](#)
- [upgrade system](#)
- [verify](#)

## boot system gateway

Specify the IP address of the default next-hop gateway for the management subnet.

<b>Syntax</b>	<code>boot system gateway ip-address</code>	
<b>Parameters</b>	<b><i>ip-address</i></b>	Enter an IP address in dotted decimal format.
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	Saving the address to the startup configuration file preserves the address in NVRAM in case the startup configuration file is deleted.	

# boot system stack-unit

Specify the location of the Dell Networking OS image to be used to boot the system.

**Syntax** `boot system stack-unit <0-5 | all> {default | primary | secondary}`

<b>Parameters</b>	<b>0-5</b>	Enter the stack member unit identifier of the stack member.
	<b>all</b>	Enter the keyword <code>all</code> to set the primary, secondary, and default images for the system.
	<b>default</b>	Enter the keyword <code>default</code> to set the default image path for the system.
	<b>primary</b>	Enter the keyword <code>primary</code> to set the primary image path for the system.
	<b>secondary</b>	Enter the keyword <code>secondary</code> to set the secondary image path for the system.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
	<b>9.4(0.0)</b>	Supported on the FN I/O aggregator.

**Usage Information** The system first attempts to load the image from the primary path. If it fails to boot, the system tries to load the image from the secondary path and if that also fails, the system loads the default image.

# cd

Change to a different working directory.

**Syntax** `cd directory`

<b>Parameters</b>	<b>directory</b>	(OPTIONAL) Enter one of the following:
		<ul style="list-style-type: none"><li>• <code>flash</code>: (internal Flash) or any sub-directory</li><li>• <code>usbflash</code>: (external Flash) or any sub-directory</li></ul>

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# copy

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

**Syntax** `copy source-file-url destination-file-url`

<b>Parameters</b>	<b>file-url</b>	Enter the following location keywords and information:
-------------------	-----------------	--

- To copy a file from the internal FLASH, enter `flash://` then the filename.
- To copy the running configuration, enter the keywords `running-config`.
- To copy the startup configuration, enter the keywords `startup-config`.
- To copy a file on the external FLASH, enter `usbflash://` then the filename.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information**

The Dell Networking OS supports a maximum of 100 files, at the root directory level, on both the internal and external Flash.

The `usbflash` commands are supported. For a list of approved USB vendors, refer to the *Dell Networking OS Release Notes*.

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.

**NOTE:** Dell Networking OS imposes a length limit on the password you create for performing the secure copy operation. Your password can be no longer than 32 characters.

For example, when using SCP, you can enter the `copy running-config scp:` command. The `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 and password, and so forth.

When you use the `copy running-config startup-config` command to copy the running configuration to the startup configuration file, Dell Networking OS creates a backup file on the internal flash of the startup configuration.

When you load the startup configuration or a configuration file from a network server such as TFTP to the running configuration, the configuration is added to the running configuration. This does not replace the existing running configuration. Commands in the configuration file has precedence over commands in the running configuration.

The Dell Networking OS supports copying the running-configuration to a TFTP server or to an FTP server:

- `copy running-config tftp:`
- `copy running-config ftp:`

**NOTE:** Dell Networking OS imposes a length limit on the password you create for accessing the FTP server. Your password can be no longer than 32 characters.

In the `copy scp: flash: example`, specifying SCP in the first position indicates that the target to specify in the ensuing prompts. Entering `flash:` in the second position means that the target is the internal Flash. In this example, the source is on a secure server running SSH, so you are prompted for the UDP port of the SSH server on the remote host.

**Example (running-config scp:)**

```
Dell#copy running-config scp:
Address or name of remote host []: 10.10.10.1
Port number of the server [22]: 99
Destination file name [startup-config]: old_running
User name to login remote host: sburgess
Password to login remote host:

Password to login remote host? dilling
```



### Example (copy scp:)

```
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
```

### Related Commands

`cd` — Changes the working directory.

## copy running-config startup-config

Copy running configuration to the startup configuration.

**Syntax** `copy running-config startup-config {duplicate}`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command is useful for quickly making a change configuration on one chassis available on external flash to move it to another chassis.

## delete

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

**Syntax** `delete flash: ([flash://]filepath) usbflash ([usbflash://]filepath)`

**Parameters**

<b>flash-url</b>	Enter the following location and keywords: <ul style="list-style-type: none"><li>For a file or directory on the internal Flash, enter <code>flash://</code> then the filename or directory name.</li><li>For a file or directory on an external USB drive, enter <code>usbflash://</code> then the filename or directory name.</li></ul>
<b>no-confirm</b>	(OPTIONAL) Enter the keywords <code>no-confirm</code> to specify that the Dell Networking OS does not require user input for each file prior to deletion.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator

# dir

Displays 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 external USB drive, enter `usbflash://` then the filename or directory name.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

```
Dell#dir
Directory of flash:

 1  drwx  4096      Jan 01 1980 00:00:00 +00:00  .
 2  drwx  2048      Mar 06 2010 00:36:21 +00:00  ..
 3  drwx  4096      Feb 25 2010 23:32:50 +00:00  TRACE_LOG_DIR
 4  drwx  4096      Feb 25 2010 23:32:50 +00:00  CORE_DUMP_DIR
 5  d---  4096      Feb 25 2010 23:32:50 +00:00  ADMIN_DIR
 6  -rwx  720969768 Mar 05 2010 03:25:40 +00:00  6gb
 7  -rwx  4260       Mar 03 2010 22:04:50 +00:00  prem-23-5-12
 8  -rwx  31969685   Mar 05 2010 17:56:26 +00:00
DellS-XL-8-3-16-148.bin
 9  -rwx  3951       Mar 06 2010 00:36:18 +00:00  startup-config

flash: 2143281152 bytes total (1389801472 bytes free)
Dell#
```

**Related Commands** `cd` — Changes the working directory.

# format flash

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** **flash memory**

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Usage Information

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

**CAUTION:** This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the `write memory` command or `copy run start` command).

### Related Commands

`copy` – copies the current configuration to either the startup-configuration file or the terminal.

`show file` – displays the contents of a text file in the local filesystem.

`show file-systems` – displays information about the file systems on the system.

## 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).

### Syntax

```
copy http://10.16.206.77/sample_file flash://sample_filecopy flash://sample_file http://10.16.206.77/sample_file
```

You can copy from the server to the switch and vice-versa.

### Parameters

<b>copy http:</b>	Address or name of remote host []: 10.16.206.77
<b>flash:</b>	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

### Supported Modes

All Modes

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Introduced on the FN I/O Aggregator.
<b>9.3(0.1)</b>	Introduced on the M I/O Aggregator.

### 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

## logging coredump stack-unit

Enable the coredump.

### Syntax

```
logging coredump stack-unit all
```

### Command Modes

CONFIGURATION

### Supported Modes

All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> <tr> <td><b>8.3.17.0</b></td> <td>Supported on the M I/O Aggregator.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.								
<b>Usage Information</b>	The Kernel core dump can be large and may take up to five to 30 minutes to upload. The Dell Networking OS does not overwrite application core dumps so delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted. The Dell Networking OS completes the coredump process and waits until the upload is complete before rebooting the system.								

## logging coredump server

Designate a server to upload core dumps.

**Syntax** `logging coredump server {ipv4-address} username name password [type] password`


<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b><i>{ipv4-address}</i></b></td> <td>Enter the server IPv4 address (A.B.C.D).</td> </tr> <tr> <td style="vertical-align: top;"><b><i>name</i></b></td> <td>Enter a username to access the target server.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>type</i></b></td> <td>Enter the password type: <ul style="list-style-type: none"> <li>• Enter 0 to enter an unencrypted password.</li> <li>• Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.</li> </ul> </td> </tr> <tr> <td style="vertical-align: top;"><b><i>password</i></b></td> <td>Enter a password to access the target server.</td> </tr> </table>	<b><i>{ipv4-address}</i></b>	Enter the server IPv4 address (A.B.C.D).	<b><i>name</i></b>	Enter a username to access the target server.	<b><i>type</i></b>	Enter the password type: <ul style="list-style-type: none"> <li>• Enter 0 to enter an unencrypted password.</li> <li>• Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.</li> </ul>	<b><i>password</i></b>	Enter a password to access the target server.
<b><i>{ipv4-address}</i></b>	Enter the server IPv4 address (A.B.C.D).								
<b><i>name</i></b>	Enter a username to access the target server.								
<b><i>type</i></b>	Enter the password type: <ul style="list-style-type: none"> <li>• Enter 0 to enter an unencrypted password.</li> <li>• Enter 7 to enter a password that has already been encrypted using a Type 7 hashing algorithm.</li> </ul>								
<b><i>password</i></b>	Enter a password to access the target server.								

**Defaults** Crash kernel files are uploaded to flash by default.

**Command Modes** CONFIGURATION

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.4.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.4.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.4.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**Usage Information** Because flash space may be limited, using this command ensures your entire crash kernel files are uploaded successfully and completely. Only a single coredump server can be configured. Configuration of a new coredump server over-writes any previously configured server.

 **NOTE:** You must disable `logging coredump` before you designate a new server destination for your core dumps.

**Related Commands** [logging coredump](#) – disables the kernel coredump

## pwd

Display the current working directory.

**Syntax** `pwd`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.
Version	Description				
<b>9.9(0.0)</b>	Introduced on the FN IOM.				

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

#### Example

```
Dell#pwd
flash:
Dell#
```

#### Related Commands

`cd` – changes the directory.

## 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://` then the filename.
- For a file on an external USB drive, enter `usbflash://` then the filename.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## restore factory-defaults

Restore factory defaults.

**Syntax** `restore factory-defaults stack-unit id {clear-all | nvram}`

#### Parameters

<b>factory-defaults</b>	Return the system to its factory default mode.
<b>id</b>	Enter the stack member unit identifier to restore the mentioned stack-unit. The range is from 0 to 6. Enter the keyword <code>all</code> to restore all units in the stack.
<b>clear-all</b>	Enter the keywords <code>clear-all</code> to reset the NvRAM and the system startup configuration.
<b>nvram</b>	Enter the keyword <code>nvram</code> to reset the NvRAM only.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## Usage Information

Restoring factory defaults deletes the existing startup configuration and all persistent settings (stacking, fanout, and so forth).

When restoring all units in a stack, all the units in the stack are placed into stand-alone mode.

When restoring a single unit in a stack, that unit placed in stand-alone mode. No other units in the stack are affected.

When restoring units in stand-alone mode, the units remain in stand-alone mode after the restoration. After the restore is complete, the units power cycle immediately.

 **CAUTION: There is no undo for this command.**

## Example

```
Dell#restore factory-defaults stack-unit 0 clear-all
*****
*Warning - Restoring factory defaults will delete the existing*
*startup-config and resets all persistent settings (stacking,*
*fanout, etc.) and boot environment variables (boot config, console*
*baud rate, management interface settings, etc.)*
*After restoration the unit(s) will be powercycled immediately.*
*Proceed with caution !*
*****

Proceed with factory settings? Confirm [yes/no]:yes

-- Restore status --
Unit  Nvram      Config      Bootvar
-----
  0    Success    Success     Success
Dell#
```

## Example (NvRAM, all)

```
Dell#restore factory-defaults stack-unit all nvram
*****
*Warning - Restoring factory defaults will delete the existing*
*persistent settings (stacking, fanout, etc.)*
*All the units in the stack will be split into standalone units.*
*After restoration the unit(s) will be powercycled immediately.*
*Proceed with caution ! *
*****

Proceed with factory settings? Confirm [yes/no]:yes

-- Restore status --
Unit Nvram      Config
-----
  0    Success
  1    Success
  2    Success
  3    Not present
  4    Not present
  5    Not present
Power-cycling the unit(s).
Dell#
```

## Example (NvRAM, single unit)

```
Dell#restore factory-defaults stack-unit 1 nvram
*****
*Warning - Restoring factory defaults will delete the existing *
*persistent settings (stacking, fanout, etc.) *
*After restoration the unit(s) will be powercycled immediately. *
*Proceed with caution ! *
*****

Proceed with factory settings? Confirm [yes/no]:yes

-- Restore status --
Unit Nvram      Config
-----
  1    Success
Power-cycling the unit(s).
Dell#
```

# show boot system

Displays information about boot images currently configured on the system.

**Syntax** `show boot system stack-unit {0-5 | all}`

**Parameters**

- 0-5** Enter this information to display the boot image information of only the entered stack-unit.
- all** Enter the keyword `all` to display the boot image information of all the stack-units in the stack.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## Example

```
Dell#show boot system stack-unit all
Current system image information in the system:
=====
Type          Boot Type          A          B
-----
Stack-unit 0 is not present.
Stack-unit 1 DOWNLOAD BOOT 9-1-0-218      9-1-0-202
Stack-unit 2 is not present.
Stack-unit 3 is not present.
Stack-unit 4 is not present.
Stack-unit 5 is not present.
```

# show file

Displays contents of a text file in the local filesystem.

**Syntax** `show file url`

**Parameters**

- url** Enter one of the following:
  - For a file on the internal Flash, enter `flash://` then the filename.
  - For a file on the external Flash, enter `usbflash://` then the filename.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## Example

```
Dell#show file flash://startup-config
! Version E8-3-17-38
```

```

boot system stack-unit 1 primary tftp://10.11.9.21/dv-m1000e-2-b2
boot system stack-unit 1 default system: A:
boot system gateway 10.11.209.62
!
hostname FTOS
--More--
Dell#

```

**Related Commands**

[format flash](#) — erases all the existing files and reformats the filesystem in the internal flash memory.  
[show file-systems](#) — displays information about the file systems on the system.

## show file-systems

Displays information about the file systems on the system.

**Syntax** `show file-systems`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example**

```

Dell#show file-systems
Size(b)      Free(b)      Feature  Type          Flags  Prefixes
2143281152   836874240   FAT32    USERFLASH    rw     flash:
-            -            -        network      rw     ftp:
-            -            -        network      rw     tftp:
-            -            -        network      rw     scp:
Dell#

```

**Command Fields**

Field	Description
<b>size(b)</b>	Lists the size in bytes of the storage location. If the location is remote, no size is listed.
<b>Free(b)</b>	Lists the available size in bytes of the storage location. If the location is remote, no size is listed.
<b>Feature</b>	Displays the formatted DOS version of the device.
<b>Type</b>	Displays the type of storage. If the location is remote, the word <code>network</code> is listed.
<b>Flags</b>	Displays the access available to the storage location. The following letters indicate the level of access: <ul style="list-style-type: none"> <li>• r = read access</li> <li>• w = write access</li> </ul>
<b>Prefixes</b>	Displays the name of the storage location.

**Related Commands**

[format flash](#) – erases all the existing files and reformats the filesystem in the internal flash memory.  
[show file](#) – displays the contents of a text file in the local filesystem.



# show os-version

Displays 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 `flash://` then the filename.
- For a file on an FTP server, enter `ftp://user:password@hostip/filepath`.
- For a file on a TFTP server, enter `tftp://hostip/filepath`.
- For a file on the external Flash, enter `usbflash://filepath` then the filename.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

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

## Example

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
-----
Platform          Version          Size             ReleaseTime
IOM-Series: XL    8-3-17-38      31603078        Jul 19 2012 06:02:28

TARGET IMAGE INFORMATION :
-----
Type              Version          Target           checksum
runtime          8-3-17-38       Control Processor passed


CPLD IMAGE INFORMATION :
-----
Card              CPLD Name        Version
Stack-unit 1     IOM SYSTEM CPLD 6
Dell#
```

# show running-config

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

**Syntax** `show running-config [entity] [configured] [status]`

**Parameters** ***entity*** (OPTIONAL) To display that entity's current (non-default) configuration, enter one of the following keywords:

 **NOTE:** If you did not configure anything for that entity, nothing displays and the prompt returns.

**boot** for the current boot configuration

<b>ftp</b>	for the current FTP configuration
<b>igmp</b>	for the current IGMP configuration
<b>interface</b>	for the current interface configuration
<b>line</b>	for the current line configuration
<b>lldp</b>	for the current lldp configuration
<b>logging</b>	for the current logging configuration
<b>management- route</b>	for the current Management port forwarding configuration
<b>monitor</b>	for the current Monitor configuration
<b>snmp</b>	for the current SNMP configuration
<b>uplink-state- group</b>	for the uplink state group configuration
<b>users</b>	for the current users configuration

**configured** (OPTIONAL) Enter the keyword *configured* to display line card interfaces with non-default configurations only.

**status** (OPTIONAL) Enter the keyword *status* to display the checksum for the running configuration and the start-up configuration.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### Example

```
Dell#show running-config
Current Configuration ...
! Version 9-4(0-180)
!
boot system stack-unit 0 primary tftp://10.11.8.12/dv-ci-stomp-tc-1-a1
!
redundancy auto-synchronize full
!
hostname Dell
...
```

#### Example

```
Dell#show running-config status

running-config bytes 5063, checksum 0xF6F801AC
startup-config bytes 4835, checksum 0x764D3787
Dell#
```

#### Example

```
Dell#sh running-config interface vlan
!
interface Vlan 1
 ip address dhcp
 mtu 2500
 no shutdown
Dell#
```

#### 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	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show startup-config
! Version E8-3-16-29
! Last configuration change at Thu Apr 26 19:19:02 2012 by default
! Startup-config last updated at Thu Apr 26 19:19:04 2012 by default
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.11.200.241/
dt-m1000e-5-c2
boot system gateway 10.11.209.254
!
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
--More--
```

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

# show version

Displays the current Dell Networking OS version information on the system.

**Syntax** show version

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

```
Dell#show version
Dell Force10 Real Time Operating System Software
Dell Force10 Operating System Version: 1.0
Dell Force10 Application Software Version: E8-3-17-38
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Thu Jul 19 05:59:59 PDT 2012
Build Path: /sites/sjc/work/swsystems01-2/ravisubramani/
ravis-8317/SW/SRC/
Cp_src/Tacacs
FTOS uptime is 4 day(s), 4 hour(s), 3 minute(s)
System image file is "dv-m1000e-2-b2" System Type: I/O-Aggregator
Control Processor: MIPS RMI XLP with 2147483648 bytes of memory.
```

```
256M bytes of boot flash memory.
1 34-port GE/TE (XL)
56 Ten GigabitEthernet/IEEE 802.3 interface(s)
```

## Command Fields

Lines	Description
<b>Beginning With</b>	
<b>Dell Force10 Network...</b>	Name of the operating system
<b>Dell Force10 Operating...</b>	OS version number
<b>Dell Force10 Application...</b>	Software version
<b>Copyright (c)...</b>	Copyright information
<b>Build Time...</b>	Software build's date stamp
<b>Build Path...</b>	Location of the software build files loaded on the system
<b>Dell Force10 uptime is...</b>	Amount of time the system has been up
<b>System image...</b>	Image file name
<b>Chassis Type:</b>	System type (M I/O Aggregator)
<b>Control Processor:...</b>	Control processor information and amount of memory on processor
<b>256M bytes...</b>	Amount of boot flash memory on the system
<b>1 34 Port</b>	Hardware configuration of the system, including the number and type of physical interfaces available

## 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: | tftp: | usbflash:} (A: | B:)`

### Parameters

<b>all</b>	Enter the keyword <code>all</code> to change both the bootflash and bootselector images.
<b>bootflash-image</b>	Enter the keywords <code>bootflash-image</code> to change the bootflash image.
<b>bootselector-image</b>	Enter the keywords <code>bootselector-image</code> to change the bootselector image.
<b>0-5</b>	Enter the keyword <code>0-5</code> to upgrade only the mentioned stack-unit.
<b>all</b>	Enter the keyword <code>all</code> to upgrade all the member stack-units.
<b>booted</b>	Enter the keyword <code>booted</code> to upgrade from the current image in the M I/O Aggregator.
<b>ftp:</b>	After entering the keyword <code>ftp:</code> , you can either 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.
<b>tftp:</b>	After entering the keyword <code>tftp:</code> , you can either 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:** After entering the keyword `flash:`, you can either follow it with the location of the source file in this form: `//filepath` or press Enter to launch a prompt sequence.
- usbflash:** After entering the keyword `usbflash:`, you can either follow it with the location of the source file in this form: `//filepath` or press Enter to launch a prompt sequence.
- A:** Enter this keyword to upgrade the bootflash partition A.
- B:** Enter this keyword to upgrade the bootflash partition B.

- Defaults** none
- Command Modes** EXEC Privilege
- Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** You must reload the 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#
```

## upgrade system

Upgrade the bootflash image or system image.

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

- Parameters**
- 0-5** Enter the keyword 0-5 to upgrade only the mentioned stack-unit.
- all** Enter the keyword `all` to upgrade all the member units of the stack.
- ftp** After entering the keyword `ftp` you can either follow it with the location of the source file in this form: `//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
- scp** After entering the keyword `scp` you can either follow it with the location of the source file in this form: `//userid:password@hostip/filepath`, or press Enter to launch a prompt sequence.
- tftp** After entering the keyword `tftp` you can either follow it with the location of the source file in this form: `//hostlocation/filepath`, or press Enter to launch a prompt sequence.
- flash** After entering the keyword `flash` you can either follow it with the location of the source file in this form: `//filepath`, or press Enter to launch a prompt sequence.
- usbflash** After entering the keyword `usbflash` you can either follow it with the location of the source file in this form: `//filepath`, or press Enter to launch a prompt sequence.
- A:** Enter this keyword to upgrade the bootflash partition A.

**B:** Enter this keyword to upgrade the bootflash partition B.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information**

You must reload Dell Networking OS after executing this command. Use the command `upgrade system stack-unit` to copy Dell Networking OS 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#
```

## 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**

<b>md5</b>	Enter the <code>md5</code> keyword to use the MD5 message-digest algorithm.
<b>sha256</b>	Enter the <code>sha256</code> keyword to use the SHA256 Secure Hash Algorithm
<b>flash://</b>	(Optional). Enter the <code>flash://</code> keyword. The default is to use the flash drive. You can just enter the image file name.
<b>img-file</b>	Enter the name the Dell Networking software image file to validate.
<b>hash-value</b>	(Optional). Enter the relevant hash published on i-Support.

**Defaults** flash drive

**Command Modes** EXEC mode

**Command History**

Version	Description
<b>9.5(0.0)</b>	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 describes control and monitoring for the I/O Aggregator.

## Topics:

- asf-mode
- asset-tag
- banner exec
- banner login
- banner motd
- clear alarms
- clear command history
- clear line
- configure
- debug cpu-traffic-stats
- debug ifm trace-flags
- debug ftpserver
- disable
- do
- enable
- exec-banner
- enable optic-info-update interval
- enable secure
- end
- exec-timeout
- exit
- feature unique-name
- ftp-server enable
- ftp-server topdir
- ftp-server username
- hostname
- http-server
- ip ftp password
- ip ftp source-interface
- ip telnet server enable
- ip telnet source-interface
- ip ftp username
- line
- login concurrent-session
- login statistics
- motd-banner
- show login statistics
- show software ifm
- ping
- reload
- service timestamps
- show alarms
- show command-history
- show configuration lock
- show cpu-traffic-stats
- show debugging



- show diag
- show environment
- show inventory
- show memory
- show processes cpu
- show processes ipc flow-control
- show processes memory
- show reset-reason
- show revision
- show server-interfaces
- show system
- show tech-support
- show uplink brief
- show util-threshold cpu
- show util-threshold memory
- ssh-peer-stack-unit
- telnet
- telnet-peer-stack-unit
- terminal length
- terminal monitor
- terminal xml
- trace route
- undebg all
- virtual-ip
- write

## asf-mode

Enable alternate store and forward (ASF) mode and forward packets as soon as a threshold is reached.

**Syntax** `asf-mode stack-unit {unit-id | all} queue size`  
 To return to standard Store and Forward mode, use the `no asf-mode stack unit` command.

**Parameters**

<b>unit-id</b>	Enter the stack member unit identifier of the stack member to reset. The range is from 0 to 5 or all.
<b>queue size</b>	Enter the queue size of the stack member. The range is from 0 to 5.

**Defaults** Not configured

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

## asset-tag

Assign and store a unique asset-tag to the stack member.

**Syntax** `asset-tag stack-unit unit id Asset-tag ID`

To remove the asset tag, use the `no stack-unit unit-id Asset-tag ID` command.

#### Parameters

- stack-unit *unit-id*** Enter the keywords `stack-unit` then the `unit-id` to assign a tag to the specific member. The range is from 0 to 5.
- Asset-tag *ID*** Enter a unique asset-tag ID to assign to the stack member. This option accepts a maximum of 10 characters, including all special characters except double quotes. To include a space in the asset-tag, enter a space within double quotes.

#### Defaults

No asset-tag is assigned.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.

#### Related Commands

`show system`— Displays the current status of all stack members or a specific member.

## banner exec

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

**Syntax** `banner exec c line c`

#### Parameters

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

#### Defaults

No banner is displayed.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

Optionally, use the `banner exec` command to create a text string that displays when you access EXEC mode. The `exec-banner` command toggles that display.

#### Example

```
Dell(conf)#banner exec ?
LINE          c banner-text(max length 255) 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: %STKUNIT0-M P:CP %SEC-5-LOGOUT: Exec session is terminated for
user on
line console
```

```

This is the banner

Dell Force10 con0 now available

Press RETURN to get started.

This is the banner

```

### Related Commands

- [banner login](#) — sets a banner for login connections to the system.
- [banner motd](#) — sets a Message of the Day banner.
- [exec-banner](#) — Enables the display of a text string when you enter EXEC mode.
- [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 {acknowledgement | 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).

<b>Parameters</b>	<b>keyboard-interactive</b>	Enter the keyword <code>keyboard-interactive</code> to require a carriage return (CR) to get the message banner prompt.
	<b>acknowledgement</b>	Enter the <code>acknowledgement</code> keyword to require a positive acknowledgement from the user while logging in to the system.
	<b>c</b>	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
	<b>line</b>	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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.10(0.0)</b>	Introduced the <code>acknowledgement</code> keyword.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** A login banner message displays only in EXEC Privilege mode after entering the `enable` command then the password. These banners do not display to users in EXEC mode.

### Example

```

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

```

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

```
$ telnet 10.11.178.16
Trying 10.11.178.16...
Connected to 10.11.178.16.
Escape character is '^]'.
THIS IS A LOGIN BANNER. PRESS 'Y' TO ACKNOWLEDGE. ACKNOWLEDGE?

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

#### Related Commands

[banner motd](#) — sets a Message of the Day banner.

[exec-banner](#) — 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`

**Parameters**

<b><i>c</i></b>	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
<b><i>line</i></b>	Enter a text string for your message of the day banner message ending the message with your delineator. The delineator is a percent character (%).

**Defaults** No banner is configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** A MOTD banner message displays only in EXEC Privilege mode after entering the `enable` command then the password. These banners do not display to users in EXEC (non-privilege) mode.

**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.

## clear alarms

Clear the alarms on the system.

**Syntax** `clear alarms`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

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

## clear command history

Clear the command history log.

**Syntax** `clear command history`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Related Commands** [show command-history](#)— displays a buffered log of all the commands all users enter along with a time stamp.

## clear line

Reset a terminal line.

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

Parameters		
<b><i>line-number</i></b>		Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
<b>console 0</b>		Enter the keywords <code>console 0</code> to reset the console port.
<b><i>vty number</i></b>		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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## configure

Enter CONFIGURATION mode from EXEC Privilege mode.

**Syntax** `configure [terminal]`

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

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### Example

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

## debug cpu-traffic-stats

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

**Syntax** `debug cpu-traffic-stats`

**Defaults** Disabled

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

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

To view the traffic statistics, use the `show cpu-traffic-stats` command.

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

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

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

## debug ifm trace-flags

Turn on the IFM internal trace-flags.

**Syntax** `debug ifm trace-flags trace-flags`

To disable this command, use the `no debug ifm trace-flags` command.

**Parameters** *trace-flags* Enter a hexadecimal number representing the trace-flag.

**Defaults** None

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

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

## debug ftpserver

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

**Syntax** `debug ftpserver`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## disable

Return to EXEC mode.

**Syntax** `disable [level]`

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

**Defaults** **1**

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## do

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

**Syntax** `do command`

**Parameters** *command* Enter an EXEC-level command.

**Defaults** none

- Command Modes**
- CONFIGURATION
  - INTERFACE

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

- Usage Information**
- The following commands are *not* supported by the `do` command:
- `enable`
  - `disable`
  - `exit`
  - `config`

**Example**

```
Dell(conf-if-te-3/1)#do clear counters
Clear counters on all interfaces [confirm]
Dell(conf-if-te-3/1)#
Dell(conf-if-te-3/1)#do clear logging
Clear logging buffer [confirm]
Dell(conf-if-te-3/1)#
Dell(conf-if-te-3/1)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
Dell(conf-if-te-3/1)#
```

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

**Defaults** **15**

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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**.

**Related Commands** [enable password](#) — configures a password for the `enable` command and to access a privilege level.



## exec-banner

Enable the display of a text string when the user enters EXEC mode.

**Syntax** `exec-banner`

**Defaults** **Enabled on all lines** (if configured, the banner appears).

**Command Modes** LINE

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Optionally, use the `banner exec` command to create a text string that is displayed when you access EXEC mode. This command toggles that display.

**Related Commands**

[banner exec](#) — configures a banner to display when entering EXEC mode.

[line](#) — enables and configures console and virtual terminal lines to the system.

## enable optic-info-update interval

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

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

To disable optical power information updates, use the `no enable optic-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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Replaces the `enable xfp-power-updates` command.

**Usage Information**

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

## enable secure

Creates configurable Full-Switch mode where Chassis Management Controller (CMC) access to FN IOM is bypassed for the elements critical to the security certifications.

**Syntax** `enable secure`

To disable the secure mode, use `no enable secure` command.

**Parameters** None

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL.

## end

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

<b>Syntax</b>	end
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONFIGURATION</li> <li>• LINE</li> <li>• INTERFACE</li> <li>• MONITOR SESSION</li> <li>• PROTOCOL LLDP</li> </ul>

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To remove the time interval, use the `exec-timeout 0 0` command.

## 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
- PROTOCOL LLDP

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Related Commands**    `end` — returns to EXEC Privilege mode.

# feature unique-name

Set a unique host name for the system.

**Syntax**            `feature unique-name`

**Defaults**            None

**Command Modes**    CONFIGURATION

**Supported Modes**

- Standalone
- VLT
- Stacking
- PMUX
- STOMP Full Switch

Command History	Version	Description
	<b>9.10(0.0)</b>	Introduced on the M I/O Aggregator, the FN IOM and MXL.

**Usage Information**

If you use the `feature unique-name` command, the system generates a host name using the platform type and system serial number. It overwrites any existing host name configured on the system using the `hostname` command. The `feature unique-name` command is also added to the running configuration.

If you disable the feature using the `no feature unique-name` command, the system reverts to the default host name of `Dell`.

If you use the `hostname` or the `no hostname` command after enabling the `feature unique-name` command, the system displays an error message stating that the `feature unique-name` is already enabled and provides an option to disable it.

**Related Commands** [hostname](#)

## ftp-server enable

Enable FTP server functions on the system.

**Syntax** `ftp-server enable`

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

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

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

## 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

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	After you enable FTP server functions with the <code>ftp-server enable</code> 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.	
<b>Related Commands</b>	<a href="#">ftp-server enable</a> — enables FTP server functions on the M I/O Aggregator. <a href="#">ftp-server username</a> — sets a username and password for incoming FTP connections to the M I/O Aggregator.	

## ftp-server username

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

<b>Syntax</b>	<code>ftp-server username username password [encryption-type] password</code>	
<b>Parameters</b>	<b><i>username</i></b>	Enter a text string up to 40 characters long as the user name.
	<b><i>password</i></b> <b><i>password</i></b>	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.
	<b><i>encryption-type</i></b>	(OPTIONAL) After the keyword <code>password</code> , enter one of the following numbers: <ul style="list-style-type: none"> <li>• 0 (zero) for an unencrypted (clear text) password</li> <li>• 7 (seven) for a hidden text password</li> </ul>
<b>Defaults</b>	Not enabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## hostname

Set the host name of the system.

<b>Syntax</b>	<code>hostname name</code>	
<b>Parameters</b>	<b><i>name</i></b>	Enter a text string, up to 32 characters long.
<b>Defaults</b>	<b>Dell Networking Operating System (OS)</b>	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information** The host name is used in the prompt.

**Related Commands** [feature unique-name](#)

## http-server

Disable / Enable the Blade I/O Manager Software.

**Syntax** `http-server blademgr`

**Parameters** **blademgr** Enter the keyword `blademgr` and specify the port for HTTP.

**Defaults** ENABLED

**Command Modes** CONFIGURATION

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

Version	Description
9.11(0.0)	Introduced on the Stomp IOA and MXL-IOA

**Usage Information** By default, the Blade I/O Manager is enabled and there is no entry in the running configuration. Using the command `no http-server blademgr`, disables the Blade I/O Manager and also a “no http-server” entry is made in the running configuration. To re-enable the Blade I/O Manager, use the command `http-server blademgr` which enables the feature and also removes the entry from the running configuration. On reload, if the system detects a “no http-server” entry in the start-config, the feature will be disabled.

 **NOTE:** Please ensure to save and reload the configuration for the changes to take effect.

## ip ftp password

Specify a password for outgoing FTP connections.

**Syntax** `ip ftp password [encryption-type] password`

**Parameters** ***encryption-type*** (OPTIONAL) Enter one of the following numbers:

- 0 (zero) for an unencrypted (clear text) password
- 7 (seven) for a hidden text password

***password*** Enter a string up to 40 characters as the password.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	The password is listed in the configuration file; you can view the password by entering the <code>show running-config ftp</code> command in EXEC mode. Use the <code>ip ftp password</code> command when you use the <code>ftp: parameter</code> in the <code>copy</code> command.
<b>Related Commands</b>	<code>copy</code> — copy files. <code>ftp-server username</code> — 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.

<b>Syntax</b>	<code>ip ftp source-interface interface</code>	
<b>Parameters</b>	<b><i>interface</i></b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383.</li> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
<b>Defaults</b>	The IP address on the system that is closest to the Telnet address is used in the outgoing packets.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<code>copy</code> — copies files from and to the switch.	

## ip telnet server enable

Enable the Telnet server on the switch.

<b>Syntax</b>	<code>ip telnet server enable</code> To disable the Telnet server, use the <code>no ip telnet server enable</code> command.	
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# ip telnet source-interface

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

**Syntax** `ip telnet source-interface interface`

**Parameters** ***interface*** Enter the following keyword and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

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

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Related Commands** [telnet](#) — telnets to another device.

# ip ftp username

Assign a user name for outgoing FTP connection requests.

**Syntax** `ip ftp username username`

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

**Defaults** No user name is configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

**Related Commands** [ip ftp password](#) — sets the password for 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 {console 0 | vty number [end-number]}`

**Parameters** **console 0** Enter the keyword `console 0` to configure the console port.



The console option is <0-0>.

**vtty number** Enter the keyword `vtty` followed by a number from 0 to 9 to configure a virtual terminal line for Telnet sessions.

The system supports 10 Telnet sessions.

**end-number** (OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure.

You can configure multiple lines at one time.

**Defaults** Not configured

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information** You cannot delete a terminal connection.

**Related Commands** [show memory](#)— View current memory usage on the M I/O Aggregator.

## login concurrent-session

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

**Syntax**

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

**Parameters**

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

**clear-line enable** Enables you to clear your existing sessions.

**Defaults** Not configured. You can use all the available sessions.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

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

Use the `login concurrent-session limit number-of-sessions` command to limit the number of concurrent sessions that any user can have on console, aux, and virtual terminal lines.

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 login 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 login, 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. You must close any of your existing sessions to login 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 days** 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 login to 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 each user on console and virtual terminal lines.

[show login statistics](#) — Displays login statistics of users who have used the console or virtual terminal lines to log in to the system.

# motd-banner

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

**Syntax** `motd-banner`

**Defaults** Enabled on all lines.

**Command Modes** LINE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# show login statistics

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

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

Parameters		
<b>all</b>	(Optional)	Displays the login statistics of all users in the last 30 days or the custom defined time period.
<b>time-period days</b>	(Optional)	Displays the number of failed login attempts by the current user in the specified period.
<b>successful-attempts</b>	(Optional)	Displays the number of successful login attempts by the current user in the last 30 days or the custom defined time period
<b>unsuccessful-attempts</b>	(Optional)	Displays the number of failed login attempts by the current user in the last 30 days or the custom defined time period.
<b>user login-id</b>	(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

**Defaults** None

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>10.10(0.0)</b>	Introduced the <code>successful-attempts</code> keyword.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

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

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

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

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

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

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

```
Dell# show login statistics user admin
-----
User: admin
Last login time: 12:52:01 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.143 )
-----
```

```

Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 0
Successful login attempt(s) in last 30 day(s): 1
-----

```

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

```

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) .

```

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

```

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

```

## Related Commands

[login statistics](#) — Enable and configure user login statistics on console and virtual terminal lines.

[login concurrent-session](#) — Configures the limit of concurrent sessions for each user on console and virtual terminal lines.

# show software ifm

Display interface management (IFM) data.

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

<b>Parameters</b>	<p><b>clients</b> Enter the keyword <code>clients</code> to display IFM client information.</p> <p><b>summary</b> (OPTIONAL) Enter the keyword <code>summary</code> to display brief information about IFM clients.</p> <p><b>ifagt number</b> Enter the keyword <code>ifagt</code> then the number of an interface agent to display software pipe and IPC statistics.</p> <p><b>ifcb interface</b> Enter the keyword <code>ifcb</code> then one of the following interface IDs then the slot/port information to display interface control block information for that interface:</p> <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10G Ethernet interface, enter the keyword <code>TenGigabitEthernet</code>.</li> </ul> <p><b>stack-unit unit-ID</b> Enter the keywords <code>stack-unit</code> then the stack member number to display IFM information for that unit. The range is from 0 to 5.</p> <p><b>trace-flags</b> Enter the keyword <code>trace-flags</code> to display IFM information for internal trace flags.</p>
-------------------	--

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```

DELL#show software ifm clients summary
ClntType Inst svcMask subSvcMask tlvSvcMask tlvSubSvc swp
IPM      0 0x00000000 0x00000000 0x90ff71f3 0xb98784a1 22
RTM      0 0x00000000 0x00000000 0x800010ff 0x0064c798 56
RIP      0 0x00000dfe 0x00000000 0x00000000 0x00000000 0
ISIS     0 0x00000002 0x00000000 0x00000000 0x00000000 0
VRRP     0 0x00000000 0x00000000 0x803330f3 0x0013c480 38
L2PM     0 0x00000000 0x00000000 0x87ff79ff 0xdb80c800 64
ACL      0 0x00000000 0x00000000 0x867f50c3 0x0103c018 81
OSPF     0 0x00000dfa 0x00100338 0x00000000 0x00000000 0
PIM      0 0x000e00f3 0x0000c000 0x00000000 0x00000000 0
IGMP     0 0x000e027f 0x00000000 0x00000000 0x00000000 0
SNMP     0 0x00000000 0x00000000 0x8000c2c0 0x00000002 21
EVTTERM  0 0x00000000 0x00000000 0x800002c0 0x0003c000 20
MRTM     0 0x00000000 0x00000000 0x81f7103f 0xc0600000 30
DSM      0 0x00000000 0x00000000 0x80771033 0x00000000 58
Mirror   0 0x00000000 0x00000000 0x80770003 0x00000000 25
LACP     0 0x00000000 0x00000000 0x8000383f 0x01000000 33
SFL_CP   0 0x00000000 0x00000000 0x807739ff 0x00000000 24
DHCP     0 0x00000000 0x00000000 0x807040f3 0x18001000 35
V6RAD    0 0x00000433 0x0000c000 0x00000000 0x00000000 0
Unidentified Client0 0x006e0002 0x00000000 0x00000000 0x00000000 0
Unidentified Client0 0x6066003f 0x00000000 0x6066003f 0x00000000 95
LLDP     0 0x007f2433 0x0408c000 0x007f2433 0x0408c000 60
--More--

```

## ping

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

**Syntax** ping *host*

**Parameters** *host* Enter the host name or the destination IP address of the device to which you are testing connectivity.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information** When you enter the ping command without specifying an IP address (Extended Ping), you are prompted for a target IP address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for Extended Commands. For information on the ICMP message codes that return from a ping command, refer to [Internet Control Message Protocol \(ICMP\) Message Types](#).

## 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#
```

## reload

Reboot the Dell Networking OS.

**Syntax** reload

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** If there is a change in the configuration, the Dell Networking OS prompts you to save the new configuration. Or you can save your running configuration with the `copy running-config` command.

**Related Commands** [reset stack-unit](#) — resets any designated stack member except the management unit.

## service timestamps

Add time stamps to debug and log messages. This command adds either the uptime or the current time and date.

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

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



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

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.14(1.5)</b>	Added support for UTC time format.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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.

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

## show alarms

Display the active major and minor alarms on the system.

**Syntax** `show alarms [threshold]`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

### Example

```
Dell# show alarms

-- Minor Alarms --
Alarm Type          Duration
-----
No minor alarms

-- Major Alarms --
Alarm Type          Duration
-----
No major alarms

Dell#
```

```
Dell# show alarms threshold

-- Temperature Limits (deg C) --
-----
Ingress-Air Off   Ingress-Air Major Off   Major Shutdown
Unit0    58        61           84           86    90
Dell#
```

# show command-history

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

**Syntax** show command-history

**Defaults** None

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Usage Information

One trace log message is generated for each command. No password information is saved to this file.

## Example

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

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

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

```
DelleMC#show command-history
[May 17 15:38:55]: CMD-(CLI):[service timestamps log datetime]by default
from console
[May 17 15:41:40]: CMD-(CLI):[write memory]by default from console
- Repeated 1 time.
[May 17 15:41:45]: CMD-(CLI):[interface tengigabitethernet 0/1]by
default from console
[May 17 15:41:47]: CMD-(CLI):[shutdown]by default from console
[May 17 15:41:50]: CMD-(CLI):[no shutdown]by default from console
[May 17 15:42:42]: CMD-(CLI):[show clock]by default from console
[May 17 15:42:52]: CMD-(CLI):[write memory]by default from console
DelleMC#
```

### Example 2: service timestamps log datetime utc

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

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

```
DelleMC# show command-history
[May 17 10:16:53]: CMD-(CLI):[service timestamps log datetime utc]by
default from console
[May 17 10:17:05]: CMD-(CLI):[show clock]by default from console
[May 17 10:17:20]: CMD-(CLI):[show running-config]by default from console
[May 17 10:17:30]: CMD-(CLI):[interface tengigabitethernet 0/2]by
default from console
[May 17 10:17:32]: CMD-(CLI):[shutdown]by default from console
[May 17 10:17:34]: CMD-(CLI):[no shutdown]by default from console
[May 17 10:17:40]: CMD-(CLI):[write memory]by default from console
```

### Example 3: service timestamps log uptime

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

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

```
DellEMC# show command-history
[1d0h24m]: CMD-(CLI):[service timestamps log uptime]by default from console
[1d0h24m]: CMD-(CLI):[interface tengigabitethernet 0/1]by default from console
[1d0h24m]: CMD-(CLI):[shutdown]by default from console
[1d0h24m]: CMD-(CLI):[no shutdown]by default from console
[1d0h25m]: CMD-(CLI):[end]by default from console
[1d0h25m]: CMD-(CLI):[write memory]by default from console
```

#### Example 4: no service timestamps log

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

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

```
DellEMC# show command-history
[May 17 15:53:44]: CMD-(CLI):[show logging]by default from console
[May 17 15:53:53]: CMD-(CLI):[show command-history]by default from console
[May 17 15:54:54]: CMD-(CLI):[end]by default from console
[May 17 15:55:00]: CMD-(CLI):[show logging]by default from console
[May 17 15:55:12]: CMD-(CLI):[show clock]by default from console
[May 17 15:55:22]: CMD-(CLI):[show running-config]by default from console
[May 17 15:55:27]: CMD-(CLI):[show command-history]by default from console
```

#### Related Commands

[clear command history](#) — clears the command history log.

## show configuration lock

Display the configuration lock status.

**Syntax** show configuration lock

**Defaults** None

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The type may be auto, manual, or rollback. When set to auto, Dell Networking OS automatically denies access to CONFIGURATION mode to all other users every time the user on the listed VTY line enters CONFIGURATION mode. When set to manual, the user on the listed VTY line must explicitly set the lock each time before entering CONFIGURATION mode. Rollback indicates that Dell Networking OS is in a rollback process. The line number shown in the output can be used to send the messages to that session or release a lock on a VTY line.

#### Example

```
Dell#show configuration lock
Configure exclusively locked by the following line:
Line          : vty 0
Line number   : 2
User          : admin
Type         : AUTO
```

```
State           : LOCKED
Ip address      : 10.11.9.97
Dell#
```

## show cpu-traffic-stats

Display the CPU traffic statistics.

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

**Parameters**

**port number** (OPTIONAL) Enter the port number to display traffic statistics on that port only. The range is from 1 to 1568.

**all** (OPTIONAL) Enter the keyword `all` to display traffic statistics on all the interfaces receiving traffic, sorted based on the traffic.


**Defaults** `all`

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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 Total packets:100
  LLC:0, SNAP:0, IP:100, ARP:0, other:0
  Unicast:100, Multicast:0, Broadcast:0
Dell#
```

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

## show debugging

View a list of all enabled debugging processes.

**Syntax** `show debugging`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

### Example

```
Dell#show debug
Generic IP: (Access List: test)
  IP packet debugging is on for (Access List: test)
  TenGigabitEthernet 0/16
  ICMP packet debugging is on for
  TenGigabitEthernet 0/16
OSPF:1
  OSPF packet debugging is on
DHCP:
  DHCP debugging is on
Dell#
```

## show diag

Display the diagnostics information.

**Syntax** `show diag {information | stack-unit number [detail | summary]] | testcase}`

Parameters	information	stack-unit <i>unit-id</i>	detail	summary	testcase
	Enter the keyword <code>information</code> to view current diagnostics information in the system.	(OPTIONAL) Enter the keywords <code>stack-unit</code> then the <code>unit-id</code> to display information on a specific stack member. The range is from 0 to 5.	(OPTIONAL) Enter the keyword <code>detail</code> to view detailed diagnostics information.	(OPTIONAL) Enter the keyword <code>summary</code> to view a summary of the diagnostics information.	Enter the keyword <code>testcase</code> to view current diagnostics testcases available in the system.

**Defaults** Summary

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## show environment

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

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

Parameters	all	stack-unit <i>unit-id</i>
	Enter the keyword <code>all</code> to view all components.	Enter the keywords <code>stack-unit</code> then the <code>unit-id</code> to display information on a specific stack member. The range is from 0 to 5.

**thermal sensor** Enter the keywords `thermal-sensor` to view all components.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example (all)**

```
Dell#show environment all

-- Unit Environment Status --
Unit Status Temp Voltage TempStatus
-----
* 1 online 66C ok 2
* Management Unit
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6 Sensor7
Sensor8 Sensor9
-----
1 51 51 63 61 61 61 67 61
64 66
Dell#
```

**Example (stack-unit)**

```
Dell#show environment stack-unit

-- Unit Environment Status --
Unit Status Temp Voltage TempStatus
-----
* 1 online 66C ok 2
* Management Unit
Dell#
```

**Example (thermal-sensor)**

```
Dell#show environment thermal-sensor

-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6 Sensor7
Sensor8 Sensor9
-----
1 51 51 64 61 61 61 67 61
64 66
Dell#
```

## show inventory

Display the switch type, components (including media), and Dell Networking OS version 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 you want to display pluggable media inventory.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

## 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 optics inserted, the output displays "Media not present or accessible".

## Example

```
Dell#show inventory
System Type       : PE-FN-410S-IOA
System Mode       : 1.0
Software Version  : 1-0(0-1859)

Unit Type  Serial Number  Part Number  Rev  Piece Part ID  Rev
Svc Tag   Exprs Svc Code
-----
* 0  PowerEdge-FN-410S-IOA  TW000000000020  07NVPVX01  X01
TW-07NVPV-00000-000-0020  X01  N/A      N/A

* - Management Unit

Software Protocol Configured
-----
DCBX
FIP Snooping
IGMP
iSCSI
LLDP
SNMP
Dell#
```

## Example (media)

```
Dell#show inventory media ?
<0-5> Slot number
| Pipe through a command

Dell#show inventory media
Slot Port  Type  Media          Serial Number  F10Qualified
-----
0  9  SFP+  10GBASE-SR    AHJ0BU3       Yes
0  10 SFP+  10GBASE-CU5M  APF125100446U1  Yes
0  11 SFP+  10GBASE-SR    CD23FM12H      Yes
0  12 SFP+  10GBASE-SR    CD23FM0XT      Yes

Dell#
```

## Related Commands

[show config \(from INTERFACE VLAN mode\)](#) — displays information on a specific physical interface or virtual interface.

# show memory

Display current memory usage on the M I/O Aggregator.

**Syntax** `show memory [stack-unit 0-5]`

**Parameters** **stack-unit 0-5** (OPTIONAL) Enter the keywords `stack-unit` then the stack unit ID of the stack member to display memory information on the designated stack member.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## Usage Information

The output for `show memory` command displays the memory usage of LP part (sysdIp) of the system. The sysdIp is an aggregate task that handles all the tasks running on the CPU.

## Example

```
Dell#show memory
Statistics On Unit 0 Processor
```

```

=====
Total (b)    Used (b)    Free (b)    Lowest (b)    Largest (b)
268435456   4010354    264425102  264375410    264425102

```

## show processes cpu

Displays CPU usage information based on processes running.

**Syntax** `show processes cpu [management-unit 1-99 [details] | stack-unit 0-5 | summary ]`

**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 `details` to display all running processes (except `sysdpl`). Refer to Example (management-unit).

**stack-unit 0-5** (OPTIONAL) Enter the keywords `stack-unit` then the stack member ID. The range is from 0 to 5.

As an option of the `show processes cpu` command, this option displays CPU usage for the designated stack member. Or, as an option of `memory`, this option limits the output of memory statistics to the designated stack member. Refer to Example (stack-unit).

**summary** (OPTIONAL) Enter the keyword `summary` to view a summary view CPU utilization of processes related to line card processing. Refer to Example (summary).

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**Example (summary)**

```

Dell#show processes cpu summary

CPU utilization   5Sec    1Min    5Min
-----
UNIT1              4%     3%     2%

```

**Example (management-unit)**

```

Dell#show processes cpu management-unit 5
CPU utilization for five seconds:4%/0%; one minute:4%; five minutes:4%
PID      Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY Process
0x00000000  2120      212      10000   3.77%  3.77%  3.77%  0 system
0x00000112  2472940   247294   10000   0.79%  0.61%  0.65%  0 sysdpl
0x000000e4  495560    49556    10000   0.20%  0.25%  0.24%  0 sysd
0x0000013d  34310     3431     10000   0.00%  0.02%  0.00%  0 lacp
0x00000121  4190      419      10000   0.00%  0.02%  0.00%  0 iscsiOpt

PID Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY Process
Dell#

```

**Example (stack-unit)**

```

Dell#show process cpu stack-unit 1
CPU utilization for five seconds:4%/0%; one minute:3%; five minutes:2%
PID      Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY Process
0x763a3000 17981680   1798168  10000   3.00%  2.67%  2.67%  0 KP
0x762ba000 0           0         0        0.00%  0.00%  0.00%  0 debugagt

```



```

0x762d9000 0 0 0 0.00% 0.00% 0.00% 0 F10StkMgr
0x762f8000 214590 21459 10000 0.00% 0.00% 0.00% 0 lcMgr
0x76319000 7890 789 10000 0.00% 0.00% 0.00% 0 dla
0x76344000 155770 15577 10000 0.00% 0.00% 0.02% 0 sysAdmTsk
0x76363000 583230 58323 10000 0.00% 0.00% 0.02% 0 timerMgr
0x76381000 658850 65885 10000 0.00% 0.17% 0.08% 0 PM
0x76299000 80110 8011 10000 0.00% 0.00% 0.00% 0 diagagt
0x763c3000 0 0 0 0.00% 0.00% 0.00% 0 evagt
--More--

```

## Related Commands

[show diag](#) — 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 stack member.

[show processes memory](#) — displays CPU usage information based on running processes.

# show processes ipc flow-control

Displays the single window protocol queue (SWPQ) statistics.

**Syntax** `show processes ipc flow-control [cp]`

**Parameters** **cp** (OPTIONAL) Enter the keyword `cp` to view the control processor's SWPQ statistics.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

Usage Information	Field	Description
	<b>Source QID /Tx Process</b>	Source Service Identifier
	<b>Destination QID/Rx Process</b>	Destination Service Identifier
	<b>Cur Len</b>	Current number of messages enqueued
	<b>High Mark</b>	Highest number of packets in the queue at any time
	<b>#of to / Timeout</b>	Timeout count
	<b>#of Retr /Retries</b>	Number of retransmissions
	<b>#msg Sent/Msg Sent/</b>	Number of messages sent
	<b>#msg Ackd/Ack Rcvd</b>	Number of messages acknowledged
	<b>Retr /Available Retra</b>	Number of retries left

Field	Description
<b>Total/ Max Retra</b>	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 queue<sup>3</sup> 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 example, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

**Example**

```
Dell#show processes ipc flow-control

Q Statistics on CP Processor
TxProcess RxProcess Cur High Time Retr Msg Ack Aval Max
          Len  Mark  Out  ies Sent  Rcvd Retra Retra ACL0 RTM0
-----
DIFFSERV0          0  0    0    0    0    0    0    10  10
ACL0      IGMP0    0  0    0    0    0    0    10  10
ACL0      PIM0    0  0    0    0    0    0    10  10
LACP0     IFMGR0  0 24    0    0    34   34   25  25
STP0      L2PM0  0  0    0    0    0    0   25  25
L2PM0     STP0    0  1    0    0    2    2   25  25
FRRP0     L2PM0  0  0    0    0    0    0   25  25
DHCP0     ACL0    0  0    0    0    0    0   25  25
DHCP0     IPMGR0  0  0    0    0    0    0   25  25
DHCP0     IFMGR0  0  0    0    0    0    0   25  25
SMUX0     IFMGR0  0 38    0    0   47   47   60  60
SMUX0     LACP0   0  1    0    0    3    3   60  60
--More--

Dell#
```

## show processes memory

Display memory usage information based on processes running in the system.

**Syntax** `show processes memory {management-unit | stack unit {0-5 | all | summary}}`

- Parameters**
- management-unit** Enter the keywords `management-unit` for CPU memory usage of the stack management unit.
  - stack unit 0-5** Enter the keywords `stack unit` then a stack unit ID of the member unit for which to display memory usage on the forwarding processor.
  - all** Enter the keyword `all` for detailed memory usage on all stack members.
  - summary** Enter the keyword `summary` for a brief summary of memory availability and usage on all stack members.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## Usage Information

show processes memory output

Field	Description
<b>Total:</b>	Total system memory available
<b>MaxUsed:</b>	Total maximum memory used ever (history indicated with time stamp)
<b>CurrentUsed:</b>	Total memory currently in use
<b>CurrentFree:</b>	Total system memory available
<b>SharedUsed:</b>	Total used shared memory
<b>SharedFree:</b>	Total free shared memory
<b>PID</b>	Process ID
<b>Process</b>	Process Name
<b>ResSize</b>	Actual resident size of the process in memory
<b>Size</b>	Process test, stack, and data size
<b>Allocs</b>	Total dynamic memory allocated
<b>Frees</b>	Total dynamic memory freed
<b>Max</b>	Maximum dynamic memory allocated
<b>Current</b>	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 the M I/O Aggregator's CP.

The output of the `show memory` command and this command differ based on which the Dell Networking OS 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:2147483648, MaxUsed:499040256, CurrentUsed:499040256,
CurrentFree:1648443392
TaskName      TotalAllocated TotalFreed MaxHeld CurrentHolding
f10appioserv  225280         0         0         192512
fcoecntrl     270336         0         0         9277440
f10appioserv  225280         0         0         192512
iscsiOpt      114688         0         0         7380992
dhclient      552960         0         0         1626112
f10appioserv  225280         0         0         192512
ndpm          618496         0         0         7389184
f10appioserv  225280         0         0         192512
vrrp          335872         0         0         7712768
f10appioserv  225280         0         0         192512
frrp          180224         0         0         7192576
f10appioserv  225280         0         0         192512
xstp         2740224         0         0         9445376
f10appioserv  225280         0         0         192512
pim          1007616         0         0         7585792
f10appioserv  225280         0         0         192512
igmp         417792         0         0         14774272
f10appioserv  225280         0         0         192512
mrtm         5496832         0         0         12636160
```

```
--More--
```

### Example (management-unit)

```
Dell#show processes memory management-unit
Total:2147483648, MaxUsed:499093504 [07/23/2012 17:42:16]
CurrentUsed:499093504, CurrentFree:1648390144
SharedUsed:18470440, SharedFree:2501104

PID Process ResSize Size Allocs Frees Max Current
633 fcoecntrl 9277440 270336 1380528 132512 1281144 1248016
289 iscsiOpt 7380992 114688 23262 16564 23262 6698
476 dhclient 1626112 552960 0 0 0 0
521 ndpm 7389184 618496 4848 0 4848 4848
160 vrrp 7712768 335872 880 0 880 880
318 frrp 7192576 180224 71086 66256 21394 4830
218 xstp 9445376 2740224 21858 0 21858 21858
277 pim 7585792 1007616 62168 0 62168 62168
--More--
```

## show reset-reason

Display the reason for the last system reboot.

**Syntax** `show reset-reason [stack-unit {stack-unit-number | all}]`

**Parameters**

- stack-unit unit-number** (OPTIONAL) Enter the keyword `stack-unit` and the stack unit number to view the reason for the last system reboot for that stack unit.
- all** (OPTIONAL) Enter the keyword `stack-unit` and the keyword `all` to view the reason for the last system reboot of all stack units in the stack.

**Command Modes**

- EXEC
- EXEC Privilege

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

Version	Description
9.14(0.0)	Introduced on the S5048F-ON.
9.13(0.0)	Introduced on the S3048-ON, S3100 series, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, C9010, MXL, M-IOA, and FN-IOM.

**Usage Information** You can use the `show reset-reason` without the `stack-unit` option to view the reason for the last system reboot of the local system.

### Example — User-initiated reboot with the reload command

```
DellEMC#show reset-reason
Cause      : Reset by User through CLI command
Reset Time: 11/05/2017-08:36
```

### Example — System reboot due to the upgrade command

```
DellEMC# show reset-reason
Cause: Reboot by Software upgrade Module.
Reset Time: 8/9/2017 1:39 PM.
```

### Example — System reboot for unknown reasons

```
DellEMC# show reset-reason
Cause: N/A
Reload Time: N/A
```

**Example — System reboot due to power loss or pressing the power button off and on.**

The example shows the reason for the last reboot as N/A for warm reset.

```
DellEMC#show reset-reason
Cause           : N/A
Reset Time      : N/A.
```

**Example — System reboot due to watchdog timeout**

```
DellEMC#show reset-reason
Cause: N/A.
Reset Time: N/A
```

**Example — System reboot due to thermal shutdown**

The example shows the reason for the last reboot as N/A for thermal shutdown.

```
DellEMC# show reset-reason
Cause: N/A
Reload Time: N/A
```

**Example — System reboot due to BIOS boot fail**

The example shows the reason for the last reboot as N/A for BIOS boot fail.

```
DellEMC#show reset-reason
Cause: NA
Reset Time: N/A.
```

**Example — Unknown reason**

If the reason for the last system reboot is not available, the system displays the reason as N/A.

```
DellEMC# show reload-reason
Cause: N/A
Time: N/A
```

**Example — Reset reason of a single stack unit**

```
DellEMC# show reset-reason stack-unit 1
Cause           : Reset by User through CLI command
Reset Time: 11/05/2017-08:36
```

**Example — Reset reason of all stack units**

```
DellEMC#show reset-reason stack-unit all
```

Last Reset Reason:

Type	Cause	Time
stack-unit 1	Reboot by Software	11/05/2017-09:04
stack-unit 2	Reboot by Software	11/05/2017-09:04
stack-unit 3	Cold Reset	N/A
stack-unit 4	N/A	N/A
stack-unit 5	N/A	N/A
stack-unit 6	N/A	N/A

## show revision

Displays the revision numbers of all stack-units.

**Syntax** `show revision`

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

**8.3.17.0**

Supported on the M I/O Aggregator.

**Example  
(Command)**

```
Dell#show revision
-- Stack unit 1 --
IOM SYSTEM CPLD : 1
Dell#
```

## show server-interfaces

Displays server port information.

**Syntax** show server-interfaces{brief|detail}

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

**Command  
History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Example (brief  
Command)**

```
Dell#show server-interfaces brief
----- show server ports brief -----
Interface OK Status Protocol Description
TenGigabitEthernet 1/1 NO up down
TenGigabitEthernet 1/2 NO up down
TenGigabitEthernet 1/3 NO up down
TenGigabitEthernet 1/4 NO up down
TenGigabitEthernet 1/5 YES up up
TenGigabitEthernet 1/6 NO up down
TenGigabitEthernet 1/7 NO up down
TenGigabitEthernet 1/8 NO up down
TenGigabitEthernet 1/9 NO up down
TenGigabitEthernet 1/10 NO up down
TenGigabitEthernet 1/11 NO up down
TenGigabitEthernet 1/12 NO up down
TenGigabitEthernet 1/13 YES up up
TenGigabitEthernet 1/14 NO up down
TenGigabitEthernet 1/15 NO up down
TenGigabitEthernet 1/16 YES up up
--More--
Dell#
```

**Example (detail  
Command)**

```
Dell#show server-interfaces detail
----- show server ports detail -----
TenGigabitEthernet 0/1 is up, line protocol is down(error-disabled[UFD])
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:99
Current address is 00:1e:c9:f1:00:99
Server Port AdminState is N/A
Pluggable media not present
Interface index is 34149121
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG130001ec9f10099
MTU 12000 bytes, IP MTU 11982 bytes
LineSpeed auto
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:59:19
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: 00:58:08
TenGigabitEthernet 0/2 is up, line protocol is down(error-disabled[UFD])
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:99
Current address is 00:1e:c9:f1:00:99
Server Port AdminState is N/A
Pluggable media not present
Interface index is 34411265
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG131001ec9f10099
--More--

```

## show system

Displays the current status of all stack members or a specific stack member.

**Syntax** `show system [brief | stack-unit unit-id]`

**Parameters**

- brief** (OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.
- stack-unit *unit-id*** (OPTIONAL) Enter the keywords `stack` `unit` then the stack member ID for information on the stack member. The range is from 0 to 5.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.11(0.0)	Included the support for Stomp B1 chipset on FN IOM.
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Example (show system brief command)**

```

Dell#show system brief

Stack MAC      : f4:8e:38:0e:e5:fc
Reload-Type    : normal-reload [Next boot : normal-reload]

-- Stack Info --
Unit UnitType  Status      ReqTyp      CurTyp      Version     Ports
-----
 0 Management  online      PE-FN-410S-IOM  PE-FN-410S-IOM  9.11(0.0)  12
 1 Member      not present
 2 Member      not present
 3 Member      not present
 4 Member      not present
 5 Member      not present
Dell#

```

### Example (stack-unit command)

```
Dell#show system stack-unit 0

-- Unit 0 --
Unit Type           : Management Unit
Status              : online
Next Boot           : online
Required Type       : PE-FN-410S-IOM - 12-port GE/TE (FN)
Current Type        : PE-FN-410S-IOM - 12-port GE/TE (FN)
Master priority     : 14
Hardware Rev        : A01
Num Ports           : 12
Up Time             : 22 min, 43 sec
Dell Networking OS Version : 9.11(0.0)
Jumbo Capable       : yes
POE Capable         : no
FIPS Mode           : disabled
Boot Flash          : A: 4.1.1.1 [booted]   B: 4.1.1.1
Boot Selector       : 4.1.0.1
Memory Size         : 2147483648 bytes
Temperature         : 55C
Voltage             : ok
Switch Power        : GOOD
Product Name        : Dell PowerEdge FN 410S IOM
Mfg By              : DELL
Mfg Date            : 2016-02-24
Serial Number       : CN282986200018
Part Number         : 0T6W0JA01
Piece Part ID       : CN-0T6W0J-28298-620-0018
PPID Revision       : A01
Service Tag         : N/A
Expr Svc Code       : N/A
Chassis Svce Tag    : 0000000
Fabric Id           : A1
Asset tag           :
PSOC FW Rev         : 0xd
ICT Test Date       : 6-2-24
ICT Test Info       : 0x0
Max Power Req       : 16896
Fabric Type         : 0x3
Fabric Maj Ver      : 0x1
Fabric Min Ver      : 0x2
SW Manageability    : 0x4
HW Manageability    : 0xd
Max Boot Time       : 3 minutes
Link Tuning         : unsupported
Auto Reboot         : enabled
Burned In MAC       : f4:8e:38:0e:e6:14
No Of MACs          : 3

Dell#
```

### Related Commands

[asset-tag](#) —Assign and store unique asset-tag to the stack member.

[show version](#) — Displays the Dell version.

[show processes memory](#) —Displays the memory usage based on the running processes.

[show diag](#) — Displays the data plane and management plane input and output statistics of a particular stack member.

## show tech-support

Displays a collection of data from other show commands, necessary for Dell Networking technical support to perform troubleshooting on Aggregators.

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



<b>Parameters</b>	<b>stack-unit</b>	(OPTIONAL) Enter the keyword <code>stack-unit</code> to view CPU memory usage for the stack member designated by <code>unit-id</code> . The range is 0 to 5.
	<b>page</b>	(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. Refer to <a href="#">CLI Basics</a> for details on filtering commands.
	<b>save</b>	Enter the keyword <code>save</code> to save the command output.  flash: Save to local flash drive ( <code>flash://filename</code> (max 20 chars))

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.14(0.0)</b>	Updated to display the <code>show revision</code> and <code>show os-version</code> command outputs.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information**

Without the `page` or `stack-unit` option, the command output is continuous, use Ctrl-z to interrupt the command output.

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 cam`
- `show clock`
- `show environment`
- `show file`
- `show interfaces`
- `show inventory`
- `show processes cpu`
- `show processes memory`
- `show running-conf`
- `show version`
- `show os-version`
- `show revision`

**Example (save)**

```
Dell#show tech-support ?
page          Page through output
stack-unit    Unit Number
|            Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 ?
page          Page through output
|            Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 | ?
except S      how 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) )
usbflash:    Save to local file system (usbflash://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:
Directory of flash:
1 drwx 4096 Jan 01 1980 01:00:00 +01:00 .
2 drwx 2048 May 16 2012 10:49:01 +01:00 ..
3 drwx 4096 Jan 24 2012 19:38:32 +01:00 TRACE_LOG_DIR
4 drwx 4096 Jan 24 2012 19:38:32 +01:00 CORE_DUMP_DIR
5 d--- 4096 Jan 24 2012 19:38:34 +01:00 ADMIN_DIR
6 -rwx 10303 Mar 15 2012 18:37:20 +01:00 startup-config.bak
7 -rwx 7366 Apr 20 2012 10:57:02 +01:00 startup-config
8 -rwx 4 Feb 19 2012 07:05:02 +01:00 dhcpBindConflict
9 -rwx 12829 Feb 18 2012 02:24:14 +01:00 startup-config.backup
10 drwx 4096 Mar 08 2012 22:58:54 +01:00 WJ_running-config
11 -rwx 7689 Feb 21 2012 04:45:40 +01:00 stbkup
flash: 2143281152 bytes total (2131476480 bytes free)
Dell

```

### Example (show tech-support)

```

Dell#show tech-support page

----- show version
-----
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 9.14(0.0RC2)
Copyright (c) 1999-2018 by Dell Inc. All Rights Reserved.
Build Time: Tue Jul 3 14:02:08 2018
Build Path: /work/swbuild01_1/build02/E9-14-0/SW/SRC
Dell Networking OS uptime is 1 day(s), 22 hour(s), 14 minute(s)

System image file is "system://A"

System Type: PE-FN-410S-IOM
Control Processor: MIPS RMI XLP with 2 Gbytes (2147483648 bytes) of
memory, core(s) 1.

128M bytes of boot flash memory.

 1 12-port GE/TE (FN)
12 Ten GigabitEthernet/IEEE 802.3 interface(s)

----- show os version
-----

RELEASE IMAGE INFORMATION :
-----
Platform          Version          Size          ReleaseTime
F-Series:FN       9.14(0.0)       45304356     May 11 2018 12:45:01

TARGET IMAGE INFORMATION :
-----
Type          Version          Target          checksum
runtime       9.14(0.0)       Control Processor  passed

BOOT IMAGE INFORMATION :
-----
Type          Version          Target          checksum
boot flash    4.1.1.1         Control Processor  passed

BOOTSEL IMAGE INFORMATION :
-----

```

```

      Type          Version          Target          checksum
boot selector      4.1.0.1          Control Processor  passed

CPLD IMAGE INFORMATION :
-----
      Card          CPLD Name      Version
Stack-unit 0      IOM SYSTEM CPLD      9

----- show revision
-----

-- Stack unit 1 --
IOM SYSTEM CPLD      : 9

----- show clock
-----
10:59:34.047 UTC Thu Jul 5 2018

<output truncated for brevity>

```

**Example (show tech-support stack-unit)**

```

Dell#show tech-support stack-unit 1
----- show version
-----
Dell Networking Real Time Operating System Software
Dell Networking Operating System Version: 1.0
Dell Networking Application Software Version: E8-3-17-38
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Thu Jul 19 05:59:59 PDT 2012
Build Path: /sites/sjc/work/swsystems01-2/ravisubramani/
ravis-8317/SW/SRC/Cp_src/
Tacacs
FTOS uptime is 4 day(s), 7 hour(s), 14 minute(s)
System image file is "dv-m1000e-2-b2"
System Type: I/O-Aggregator
Control Processor: MIPS RMI XLP with 2147483648 bytes of memory.
256M bytes of boot flash memory.
1 34-port GE/TE (XL)
56 Ten GigabitEthernet/IEEE 802.3 interface(s)
----- show clock
-----
17:49:37.2 UTC Mon Jul 23 2012
----- show running-config
-----
Current Configuration ...
! Version E8-3-17-38
! Last configuration change at Mon Jul 23 17:10:18 2012 by default
!
boot system stack-unit 1 primary tftp://10.11.9.21/dv-m1000e-2-b2
boot system stack-unit 1 default system: A:
boot system gateway 10.11.209.62
!
redundancy auto-synchronize full
!
service timestamps log datetime
!
hostname FTOS
----- show ip management route
-----
Destination Gateway State
-----
1
--More--
Dell#

```

**Related Commands**

- [show version](#) — displays the Dell Networking OS version.
- [show system](#) — displays the current switch status..
- [show environment](#) — displays system component status.
- [show processes memory](#) — displays memory usage based on the running processes.

# show uplink brief

Displays the uplink port information.

**Syntax** show uplink {brief|detail}

**Parameters**

- brief** Enter the keyword `brief` to display a brief summary of the uplink port information.
- detail** Enter the keyword `detail` to display uplink port information with description.

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example (brief)

```
Dell#show uplink brief
----- show uplink brief -----
Interface          OK Status   Protocol Description
TenGigabitEthernet 0/41 NO up      down
TenGigabitEthernet 0/43 NO up      down
TenGigabitEthernet 0/44 NO up      down
TenGigabitEthernet 0/45 NO up      down
TenGigabitEthernet 0/46 NO up      down
TenGigabitEthernet 0/47 NO up      down
TenGigabitEthernet 0/48 NO up      down
TenGigabitEthernet 0/49 NO up      down
TenGigabitEthernet 0/50 NO up      down
TenGigabitEthernet 0/51 NO up      down
TenGigabitEthernet 0/52 NO up      down
TenGigabitEthernet 0/53 NO up      down
TenGigabitEthernet 0/54 NO up      down
TenGigabitEthernet 0/55 NO up      down
TenGigabitEthernet 0/56 NO up      down
TenGigabitEthernet 1/41 NO up      down
TenGigabitEthernet 1/42 NO up      down
TenGigabitEthernet 1/43 NO up      down
--More--
4 www.force10networks.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
Dell#
```

## Example (detail)

```
Dell#show uplink detail
----- show uplink detail -----
TenGigabitEthernet 0/41 is up, line protocol is down
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:99
Current address is 00:1e:c9:f1:00:99
Port is not present
Pluggable media not present
Interface index is 44634881
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG170001ec9f10099
MTU 12000 bytes, IP MTU 11982 bytes
LineSpeed auto
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 2d19h53m
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
--More--
```

## show util-threshold cpu

Displays the set CPU utilization threshold values.

**Syntax** `show util-threshold cpu`

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command displays all CPU utilization thresholds of the management, standby, and stack-units.

## show util-threshold memory

Displays the set memory utilization threshold values.

**Syntax** `show util-threshold memory`

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command displays all memory utilization thresholds of the management, standby, and stack-units.

## ssh-peer-stack-unit

Open an SSH connection to the peer stack-unit.

**Syntax** `ssh-peer-stack-unit [-| username]`

**Parameters** `-| username` (OPTIONAL) Enter the keyword `-|` followed by your username.  
Default: The username associated with the terminal.

**Defaults** Not configured.

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## telnet

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

**Syntax** `telnet {host | ip-address [/source-interface]}`

Parameters	Parameter	Description
	<b>host</b>	Enter the name of a server.
	<b>ip-address</b>	Enter the IPv4 address in dotted decimal format of the server.
	<b>source-interface</b>	(OPTIONAL) Enter the keywords <code>/source-interface</code> then the interface information to include the source interface. Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>

**Defaults** Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** Telnet to link-local addresses is not supported.

## telnet-peer-stack-unit

Open a telnet connection to the peer stack-unit.

**Syntax** `telnet-peer-stack-unit`

**Defaults** Not configured.

**Command Modes**

- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# terminal length

Configure the number of lines displayed on the terminal screen.

**Syntax** `terminal length screen-length`  
To return to the default values, use the `no terminal length` command.

**Parameters** *screen-length* Enter a number of lines. Entering zero will cause the terminal to display without pausing. The range is from 0 to 512.  
Default: 24 lines

**Defaults** 24 lines

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

# terminal monitor

Configure the Dell Networking OS to display messages on the monitor/terminal.

**Syntax** `terminal monitor`  
To return to default settings, use the `no terminal monitor` command.

**Defaults** Disabled

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

# terminal xml

Enable XML mode in Telnet and SSH client sessions.

**Syntax** `terminal xml`  
To exit the XML mode, use the `no terminal monitor` command.

**Defaults** Disabled

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command enables XML input mode where you can either cut and paste XML requests or enter the XML requests line-by-line.

## trace route

View the packet path to a specific device.

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

**Parameters**

- host** Enter the name of device.
- ip-address** Enter the IP address of the device in dotted decimal format.

**Defaults** Timeout = 5 seconds; Probe count = 3; 30 hops max; 40 byte packet size; UDP port = 33434

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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.

### Example (IPv4)

```
Dell#traceroute www.force10networks.com
Translating "www.force10networks.com"...domain server (10.11.0.1)
[OK]
Type Ctrl-C to abort.
-----
Tracing the route to www.force10networks.com (10.11.84.18),
 30 hops max, 40 byte packets
-----
TTL Hostname Probe1 Probe2 Probe3
 1 10.11.199.190 001.000 ms 001.000 ms 002.000 ms
 2 gwegress-sjc-02.force10networks.com (10.11.30.126)
   005.000 ms 001.000 ms 001.000 ms
 3 fw-sjc-01.force10networks.com (10.11.127.254)
   000.000 ms 000.000 ms 000.000 ms
 4 www.force10networks.com (10.11.84.18)
   000.000 ms 000.000 ms 000.000 ms
Dell#
```

### Related Commands

## undebug all

Disable all debug operations on the system.

**Syntax** `undebug all`



**Defaults** none  
**Command Modes** • EXEC Privilege  
**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## virtual-ip

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

**Syntax** `virtual-ip {ipv4-address}`

**Parameters** **ipv4-address** Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.).

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Each time you issue this command, it replaces the previously configured address of the same family. 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, the IPv4 virtual addresses are removed.

### Example

```
Dell#virtual-ip 10.11.197.99/16
```

## write

Copy the current configuration to either the startup-configuration file or the terminal.

**Syntax** `write {memory | terminal}`

**Parameters**

- memory** Enter the keyword `memory` to copy the current running configuration to the startup configuration file. This command is similar to the `copy running-config startup-config` command.
- terminal** Enter the keyword `terminal` to copy the current running configuration to the terminal. This command is similar to the `show running-config` command.

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

**Command History****Version****Description****9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

**8.3.17.0**

Supported on the M I/O Aggregator.

**Usage Information**

The `write memory` command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named "startup-configuration", the running-config is not saved to that file; 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

The system limits network access for certain users by using virtual local area network (VLAN) assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- If no VLAN is supplied by the RADIUS server or if you disable 802.1X authorization, the port configures in its access VLAN after successful authentication.
- If you enable 802.1X authorization but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This safeguard prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If you enable 802.1X authorization and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If you enable port security on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If you disable 802.1X on the port, it returns to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

### Topics:

- [debug dot1x](#)
- [dot1x authentication \(Configuration\)](#)
- [dot1x authentication \(Interface\)](#)
- [dot1x auth-fail-vlan](#)
- [dot1x auth-server](#)
- [dot1x auth-type mab-only](#)
- [dot1x guest-vlan](#)
- [dot1x host-mode](#)
- [dot1x mac-auth-bypass](#)
- [dot1x max-eap-req](#)
- [dot1x max-suplicants](#)
- [dot1x port-control](#)
- [dot1x quiet-period](#)
- [dot1x reauthentication](#)
- [dot1x reauth-max](#)
- [dot1x server-timeout](#)
- [dot1x supplicant-timeout](#)
- [dot1x tx-period](#)
- [show dot1x cos-mapping interface](#)
- [show dot1x interface](#)

# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## dot1x authentication (Configuration)

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

**Syntax** `dot1x authentication`  
To disable dot1x on a globally, use the `no dot1x authentication` command.

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [dot1x authentication \(Configuration\)](#) — Enable dot1x globally.

## 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**

<b><i>vlan-id</i></b>	Enter the VLAN Identifier. The range is from 1 to 4094.
<b>max-attempts <i>number</i></b>	(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 <b>3</b> .

**Defaults** 3 attempts

**Command Modes** CONFIGURATION (*conf-if-interface-slot/port*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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](#) — Enables port control on an interface.
- [dot1x guest-vlan](#) — Configures a guest VLAN for limited access users or for devices that are not 802.1X capable.
- [show dot1x interface](#) — Displays 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# dot1x auth-type mab-only

To authenticate a device with MAC authentication bypass (MAB), only use the host MAC address.

**Syntax** `dot1x auth-type mab-only`

**Defaults** Disabled

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The prerequisites for enabling MAB-only authentication on a port are:

- Enable 802.1X authentication globally on the switch and on the port (the `dot1x authentication` command).
- Enable MAC authentication bypass on the port (the `dot1x mac-auth-bypass` command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1x authentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the `no dot1x auth-type mab-only` command.

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

# 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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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](#) — Configures an authentication failure VLAN.
- [dot1x reauthentication](#) — Enables 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**

<b>single-host</b>	Enable single-host authentication.
<b>multi-host</b>	Enable multi-host authentication.
<b>multi-auth</b>	Enable multi-supPLICANT authentication.

**Defaults** **single-host**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## dot1x max-eap-req

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

<b>Syntax</b>	<code>dot1x max-eap-req <i>number</i></code> To return to the default, use the <code>no dot1x max-eap-req</code> command.	
<b>Parameters</b>	<b><i>number</i></b>	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 <b>2</b> .
<b>Defaults</b>	<b>2</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

<b>Syntax</b>	<code>dot1x max-suplicants <i>number</i></code>	
<b>Parameters</b>	<b><i>number</i></b>	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 <b>128</b> .
<b>Defaults</b>	128 hosts can be authenticated on a single authenticator port.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">dot1x host-mode</a> — Enables single-host or multi-host authentication.	

## dot1x port-control

Enable port control on an interface.

<b>Syntax</b>	<code>dot1x port-control {force-authorized   auto   force-unauthorized}</code>	
<b>Parameters</b>	<b>force-authorized</b>	Enter the keywords <code>force-authorized</code> to forcibly authorize a port.
	<b>auto</b>	Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.
	<b>force-unauthorized</b>	Enter the keywords <code>force-unauthorized</code> to forcibly deauthorize a port.
<b>Defaults</b>	none	



**Command Modes** Auto

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The authenticator completes 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 **60**.

**Defaults** **60** seconds

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 `interval` then the interval time, in seconds, after which reauthentication is initiated. The range is from 1 to 31536000 (one year). The default is **3600** (1 hour).

**Defaults** **3600** seconds (1 hour)

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## dot1x reauth-max

Configure the maximum number of times a port can reauthenticate 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 reauthentications. The range is from 1 to 10. The default is **2**.

**Defaults** **2**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you configure the `dot1x server-timeout` value, take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the `dot1x server-timeout` value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula: `dot1x server-timeout seconds > (radius-server retransmit seconds + 1) * radius-server timeout seconds`.

Where the default values are as follows: `dot1x server-timeout` (30 seconds), `radius-server retransmit` (3 seconds), and `radius-server timeout` (5 seconds).

For example:

```
Dell(conf)#radius-server host 10.11.197.105 timeout 6
Dell(conf)#radius-server host 10.11.197.105 retransmit 4
Dell(conf)#interface tengigabitethernet 2/1
Dell(conf-if-te-2/1)#dot1x server-timeout 40
```

# dot1x supplicant-timeout

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

<b>Syntax</b>	<code>dot1x supplicant-timeout seconds</code> To return to the default, use the <code>no dot1x supplicant-timeout</code> command.	
<b>Parameters</b>	<b>seconds</b>	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is <b>30</b> .
<b>Defaults</b>	<b>30</b> seconds	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# dot1x tx-period

Configure the intervals at which EAPOL PDUs the Authenticator PAE transmits.

<b>Syntax</b>	<code>dot1x tx-period seconds</code> To return to the default, use the <code>no dot1x tx-period</code> command.	
<b>Parameters</b>	<b>seconds</b>	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535. The default is <b>30</b> .
<b>Defaults</b>	<b>30</b> seconds	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# 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.

<b>Syntax</b>	<code>show dot1x cos-mapping interface interface [mac-address mac-address]</code>	
<b>Parameters</b>	<b>interface</b>	Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>For a Ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul>
	<b>mac-address</b>	(Optional) MAC address of an 802.1X-authenticated supplicant.
<b>Defaults</b>	none	
<b>Command Modes</b>	• EXEC	

- EXEC privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

To display CoS mapping information only for the specified supplicant, enter a supplicant's MAC address using the `mac-address` option.

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 0/1

802.1p CoS re-map table on Te 0/1:
-----
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 0/1 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 0/1:
-----

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**

- interface*** Enter one of the following keywords and slot/port or number information:
  - For a Ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- mac-address*** (Optional) MAC address of a supplicant.

**Defaults** none

**Command Modes**

- EXEC
- EXEC privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you enable 802.1X multi-supplicant authentication on a port, additional 802.1X configuration details (Port Authentication status, Untagged VLAN ID, Authentication PAE state, and Backend state) are displayed for each supplicant, as shown in the following example.

**Example**

```
Dell#show dot1x interface tengigabitethernet 0/1

802.1x information on Te 0/1:
-----
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#

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

802.1x information on Te 0/1:
-----
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#
```

# Access Control Lists (ACL)

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

The 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](#)

 **NOTE:** For ACL commands that use the Trace function, refer to the [Secure DHCP Commands](#) section in the [Security](#) chapter.

## Topics:

- [Commands Common to all ACL Types](#)
- [description](#)
- [remark](#)
- [resequence access-list](#)
- [resequence prefix-list ipv4](#)
- [show config](#)
- [Common IP ACL Commands](#)
- [access-class](#)
- [clear counters ip access-group](#)
- [ip access-group](#)
- [show ip access-lists](#)
- [show ip accounting access-list](#)
- [Standard IP ACL Commands](#)
- [ip access-list standard](#)
- [permit \(for Standard IP ACLs\)](#)
- [seq](#)
- [Extended IP ACL Commands](#)
- [deny \(for Extended IP ACLs\)](#)
- [deny icmp](#)
- [deny tcp](#)
- [deny udp](#)
- [ip access-list extended](#)
- [permit \(for Extended IP ACLs\)](#)
- [permit icmp](#)
- [permit tcp](#)
- [permit udp](#)
- [seq](#)
- [Common MAC Access List Commands](#)
- [clear counters mac access-group](#)
- [mac access-group](#)
- [show mac access-lists](#)
- [show mac accounting access-list](#)
- [Standard MAC ACL Commands](#)

- deny
- deny
- mac access-list extended
- permit
- seq
- Extended MAC ACL Commands
- mac access-list standard
- permit
- seq
- IP Prefix List Commands
- clear ip prefix-list
- deny
- ip prefix-list
- permit
- seq
- show config
- show ip prefix-list detail
- show ip prefix-list summary
- Route Map Commands
- continue
- description
- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag
- route-map
- set automatic-tag
- set metric
- set metric-type
- set tag
- show config
- show route-map
- deny (for Standard IP ACLs)
- deny
- seq
- deny tcp
- deny udp
- deny arp (for Extended MAC ACLs)
- deny icmp
- deny ether-type (for Extended MAC ACLs)
- deny
- deny
- permit (for Standard IP ACLs)
- permit
- permit ether-type (for Extended MAC ACLs)
- permit icmp
- permit udp
- permit (for Extended IP ACLs)
- permit
- seq
- permit tcp
- seq arp
- seq ether-type



- seq
- seq
- permit udp
- permit tcp
- permit icmp
- permit
- deny udp (for IPv6 ACLs)
- deny tcp (for IPv6 ACLs)
- deny icmp (for Extended IPv6 ACLs)
- deny (for 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` command).


### description

Configure a short text string describing the ACL.

<b>Syntax</b>	<code>description text</code>	
<b>Parameters</b>	<b><i>text</i></b>	Enter a text string up to 80 characters long.
<b>Defaults</b>	Not enabled.	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONFIGURATION-IP ACCESS-LIST-STANDARD</li> <li>• CONFIGURATION-IP ACCESS-LIST-EXTENDED</li> <li>• CONFIGURATION-MAC ACCESS LIST-STANDARD</li> <li>• CONFIGURATION-MAC ACCESS LIST-EXTENDED</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### remark

Enter a description for an ACL entry.

<b>Syntax</b>	<code>remark [remark-number] [description]</code>	
<b>Parameters</b>	<b><i>remark-number</i></b>	Enter the remark number. The range is from 0 to 4294967290.
		 <b>NOTE:</b> You can use the same sequence number for the remark and an ACL rule.
	<b><i>description</i></b>	Enter a description of up to 80 characters.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONFIGURATION-IP ACCESS-LIST-STANDARD</li> <li>• CONFIGURATION-IP ACCESS-LIST-EXTENDED</li> <li>• CONFIGURATION-MAC ACCESS LIST-STANDARD</li> <li>• CONFIGURATION-MAC ACCESS LIST-EXTENDED</li> </ul>	

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.14.0.0</b>	Made the remark number as an optional value.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

You can include a remark with or without a remark number. If you do not enter a remark number, the remark inherits the sequence number of the last ACL rule. If there is no ACL rule when you enter a remark, the remark takes sequence number 5. If you configure two remarks with the same sequence number and different strings, the second one replaces the first string. You cannot configure two or more remarks with the same string and different sequence numbers.

To remove a remark, use the `no remark` command with or without the sequence number. If there is a matching string, the system deletes the remark.

### Example

```
DelleMC(config-std-nacl)# remark 10 Deny rest of the traffic
DelleMC(config-std-nacl)# remark 5 Permit traffic from XYZ Inc.
DelleMC(config-std-nacl)# show config
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 deny any
DelleMC(config-std-nacl)#
```

The following example shows adding a remark without a sequence number:

```
DELLEMC(config-ext-nacl)#permit ip any any
DELLEMC(config-ext-nacl)#remark permit any ip
DELLEMC(config-ext-nacl)#show c
!
ip access-list extended testac
seq 5 permit ip any any
remark 5 permit any ip
```

The following example shows that the system displays an error message when the same remark string is used with different remark numbers.

```
DELLEMC(config-ext-nacl)#seq 100 permit ip any any
DELLEMC(config-ext-nacl)#remark 10 permit any ip
DELLEMC(config-ext-nacl)#remark permit any ip
DELLEMC(config-ext-nacl)#% Error : Remark string already exists
```

**Related Commands** [resequence access-list](#) — Re-assigns sequence numbers to entries of an existing access-list.

## 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}`

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

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing access-list.

**Related Commands** [resequence prefix-list ipv4](#) — resequences a prefix list.

## resequence prefix-list ipv4

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

**Syntax** `resequence prefix-list ipv4 {prefix-list-name StartingSeqNum Step-to-increment}`

<b>Parameters</b>	<b><i>prefix-list-name</i></b>	Enter the name of the configured prefix list, up to 140 characters long.
	<b><i>StartingSeqNum</i></b>	Enter the starting sequence number to resequence. The range is from 0 to 65535.
	<b><i>Step-to-Increment</i></b>	Enter the step to increment the sequence number. The range is from 1 to 65535.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

**Related Commands** [seq](#) — Assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

# show config

Display the current ACL configuration.

**Syntax** `show config`

- Command Modes**
- CONFIGURATION-IP ACCESS-LIST-STANDARD
  - CONFIGURATION-IP ACCESS-LIST-EXTENDED
  - CONFIGURATION-MAC ACCESS LIST-STANDARD
  - CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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 switch 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]`

- Parameters**
- access-list-name** Enter the name of a configured Standard ACL, up to 140 characters.
  - ipv4** Enter the keyword `ipv4` to configure an IPv4 access class.
  - ipv6** Enter the keyword `ipv6` to configure an IPv6 access class.

**Defaults** Not configured.

**Command Modes** LINE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Added the <code>ipv4</code> and <code>ipv6</code> parameters to the command.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 is a generic way of configuring access restrictions.

To be able to filter access exclusively using either IPv4 or IPv6 rules, you must 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, you must 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, you must 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** **access-list-name** (OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## ip access-group

Apply an egress IP ACL to an interface.

**Syntax** `ip access-group access-list-name {in | out} [implicit-permit] [vlan vlan-id] [layer3]`

**Parameters**

- access-list-name** Enter the name of a configured access list, up to 140 characters.
- in** Enter the keyword `in` to apply the ACL to incoming traffic.
- out** Enter the keyword `out` to apply the ACL to the outgoing traffic.
- implicit-permit** (OPTIONAL) Enter the keyword `implicit-permit` to change the default action of the ACL from `implicit-deny` to `implicit-permit` (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
- vlan vlan-id** (OPTIONAL) Enter the keyword `vlan` then the ID numbers of the VLANs.
- layer3** (OPTIONAL) Enter the keyword `layer3` to enable layer 3 mode. It ensures that all the ACL rules in the access-group are applied only for L3 router packets.


**Defaults** Not enabled..


**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information** You can assign one ACL (standard or extended ACL) to an interface..

 **NOTE:** This command is *not* supported on the FN IOMSwitch Loopback interfaces.

 **NOTE:** If outbound(egress) IP ACL is applied on switch port, filter will be applied only for routed traffic egressing out of that port.

**Related Commands**

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

## show ip access-lists

Display all of the IP 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 ip access-lists [access-list-name] [interface interface] [in]`

**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 or number information:
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- in** Identify whether ACL is applied on the ingress or egress side.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ip access-lists test in
Standard Ingress IP access list test
seq 5 permit 1.1.1.0/24 count (0 packets)
seq 10 deny 2.1.1.0/24 count (0 packets)
```

## 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`

**Parameters**

- access-list-name** Enter the name of the ACL to be displayed.

**cam\_count** List the count of the CAM rules for this ACL.

**interface**  
**interface** Enter the keyword `interface` then the one of the following keywords and slot/port or number information:

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

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.


Usage Information	show ip accounting access-lists Field	Description
	“Extended IP...”	Displays the name of the IP ACL.
	“seq 5...”	Displays the filter. If the keywords <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
!
Standard Ingress IP access list test on TenGigabitEthernet 0/1
Total cam count 2
seq 5 permit 1.1.1.0/24 count (0 packets)
seq 10 deny 2.1.1.0/24 count (0 packets)
```

## 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 switch supports both Ingress and Egress IP ACLs.

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

## ip access-list standard

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

**Syntax** `ip access-list standard access-list-name`

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

**Defaults** All IP access lists contain an implicit `deny any`, that is, if no match occurs, the packet is dropped.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>The Dell operating system supports one ingress and one egress IP ACL per interface.</p> <p>The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.</p>						
<b>Example</b>	<pre>Dell(conf)#ip access-list standard TestList Dell(config-std-nacl)#</pre>						
<b>Related Commands</b>	<p><a href="#">ip access-list extended</a> — creates an extended access list.</p> <p><a href="#">resequence access-list</a> — Displays the current configuration.</p>						

## 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} [no-drop] [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.

<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b>source</b></td> <td>Enter the IP address in dotted decimal format of the network from which the packet was sent.</td> </tr> <tr> <td style="vertical-align: top;"><b>mask</b></td> <td>(OPTIONAL) Enter a network <code>mask</code> 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.</td> </tr> <tr> <td style="vertical-align: top;"><b>any</b></td> <td>Enter the keyword <code>any</code> to specify that all routes are subject to the filter.</td> </tr> <tr> <td style="vertical-align: top;"><b>host ip-address</b></td> <td>Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.</td> </tr> <tr> <td style="vertical-align: top;"><b>no-drop</b></td> <td>Enter the keywords <code>no-drop</code> to match only the forwarded packets.</td> </tr> <tr> <td style="vertical-align: top;"><b>count</b></td> <td>(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.</td> </tr> <tr> <td style="vertical-align: top;"><b>bytes</b></td> <td>(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.</td> </tr> <tr> <td style="vertical-align: top;"><b>dscp</b></td> <td>(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DCSCP values.</td> </tr> <tr> <td style="vertical-align: top;"><b>order</b></td> <td>(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 (<b>255</b>).</td> </tr> <tr> <td style="vertical-align: top;"><b>fragments</b></td> <td>Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.</td> </tr> <tr> <td style="vertical-align: top;"><b>log</b></td> <td>(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.</td> </tr> <tr> <td style="vertical-align: top;"><b>threshold-in-msgs count</b></td> <td>(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.</td> </tr> <tr> <td style="vertical-align: top;"><b>interval minutes</b></td> <td>(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.</td> </tr> </table>	<b>source</b>	Enter the IP address in dotted decimal format of the network from which the packet was sent.	<b>mask</b>	(OPTIONAL) Enter a network <code>mask</code> 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.	<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.	<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.	<b>no-drop</b>	Enter the keywords <code>no-drop</code> to match only the forwarded packets.	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.	<b>bytes</b>	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.	<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DCSCP values.	<b>order</b>	(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 ( <b>255</b> ).	<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.	<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.	<b>threshold-in-msgs count</b>	(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.	<b>interval minutes</b>	(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.
<b>source</b>	Enter the IP address in dotted decimal format of the network from which the packet was sent.																										
<b>mask</b>	(OPTIONAL) Enter a network <code>mask</code> 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.																										
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.																										
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.																										
<b>no-drop</b>	Enter the keywords <code>no-drop</code> to match only the forwarded packets.																										
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.																										
<b>bytes</b>	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.																										
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DCSCP values.																										
<b>order</b>	(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 ( <b>255</b> ).																										
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.																										
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.																										
<b>threshold-in-msgs count</b>	(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.																										
<b>interval minutes</b>	(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

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the 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).

**Related Commands**

[deny](#) — assigns a IP ACL filter to deny IP packets.  
[ip access-list standard](#) — creates a standard ACL.

## 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} {source [mask] | any | host ip-address} [count [byte] [dscp value] [order] [fragments] [threshold-in-msgs [count]]`

**Parameters**

<b>sequence-number</b>	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
<b>deny</b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
<b>permit</b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
<b>source</b>	Enter an IP address in dotted decimal format of the network from which the packet was received.

<b>mask</b>	(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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.

**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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

When 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` — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

## 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 switch 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 (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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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).
<b>monitor</b>	(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.
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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 *minutes*** (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.

**monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults** By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes** CONFIGURATION-EXTENDED-ACCESS-LIST

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

#### 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.

## 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][threshold-in-msgs] [count]]
```

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.

<b>Parameters</b>	<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
	<b>mask</b>	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.
	<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
	<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
	<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
	<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
	<b>order</b>	(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).
	<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.	

**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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
	<b>9.3(0.0)</b>	Added the support for logging ACLs on the MXL 10/40GbE Switch IO Module.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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

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] [threshold-in-msgs [count]]`

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

<b>source</b>	Enter the IP address of the network or host from which the packets are sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>bit</b>	Enter a flag or combination of bits: <ul style="list-style-type: none"><li>• <code>ack</code>: acknowledgement field</li><li>• <code>fin</code>: finish (no more data from the user)</li><li>• <code>psh</code>: push function</li><li>• <code>rst</code>: reset the connection</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>urg</code>: urgent field</li></ul>
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li></ul>
<b>port port</b>	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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li><li>• 169 = SNMP</li></ul>
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

**threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

### 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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### 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*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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).

### Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Dell#	Data	Mask	From	To	#Covered
1	00001111110100000	11111111111100000	4000	4031	32
2	00001111111000000	11111111111000000	4032	4095	64
3	00010000000000000	11111000000000000	4096	6143	2048
4	00011000000000000	11111100000000000	6144	7167	1024
5	00011100000000000	11111110000000000	7168	7679	512
6	00011110000000000	11111111000000000	7680	7935	256
7	00011111000000000	11111111110000000	7936	7999	64
8	00011111010000000	11111111111111111	8000	8000	1

```
Total Ports: 4001
```

### Example

An ACL rule with a TCP port 1023 uses only one entry in the CAM.

```
Dell# 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] [threshold-in-msgs [count]]
```

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li></ul>
<b>port port</b>	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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 ( <b>255</b> ).



**fragments** Enter the keyword `fragments` to use ACLs to control packet fragments.

**threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword then a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs are terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

**Defaults** By default 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which the ACL logs are generated is five minutes.

**Command Modes** CONFIGURATION-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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

**Example** An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```

Dell# 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.

```

Dell# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Example**

```
Dell(conf)#ip access-list extended TESTListEXTEND
Dell(config-ext-nacl)#
```

**Related Commands** [ip access-list standard](#) — configures a standard IP access list.  
[resequence access-list](#) — Displays the current configuration.

## 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		
<b>source</b>		Enter the IP address in dotted decimal format of the network from which the packet was sent.
<b>mask</b>	(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.
<b>any</b>		Enter the keyword <i>any</i> to specify that all routes are subject to the filter.
<b>host ip-address</b>		Enter the keyword <i>host</i> then the IP address to specify a host IP address or hostname.
<b>count</b>	(OPTIONAL)	Enter the keyword <i>count</i> to count packets processed by the filter.
<b>bytes</b>	(OPTIONAL)	Enter the keyword <i>bytes</i> to count bytes processed by the filter.

<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

**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 tcp](#) — assigns a permit filter for TCP packets.
- [permit udp](#) — assigns a permit filter for UDP packets.

# permit icmp

Configure a filter to allow all or specific ICMP messages.

**Syntax** `permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} [dscp] [message-type] [count [byte]] [order] [fragments] [threshold-in-msgs [count]]`

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is 0 to 63.
<b>message-type</b>	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in-msgs count</b>	(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.

## 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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 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 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][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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>bit</b>	Enter a flag or combination of bits: <ul style="list-style-type: none"><li>• <code>ack</code>: acknowledgement field</li><li>• <code>fin</code>: finish (no more data from the user)</li><li>• <code>psh</code>: push function</li><li>• <code>rst</code>: reset the connection</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>urg</code>: urgent field</li></ul>
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li></ul>

- `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.

***log*** (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

***threshold-in msgs count*** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

***interval minutes*** (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.

***monitor*** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**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 switch cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

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.

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).

### Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# 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 1023 uses only one entry in the CAM.

```
Dell# 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] [threshold-in-msgs [count]]
```

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.

<b>Parameters</b>	<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
	<b>mask</b>	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.
	<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
	<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
	<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"> <li>• <code>eq</code> = equal to</li> <li>• <code>neq</code> = not equal to</li> <li>• <code>gt</code> = greater than</li> <li>• <code>lt</code> = less than</li> <li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter)</li> </ul>
	<b>port port</b>	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.
	<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
	<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
	<b>order</b>	(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 ( <b>255</b> ).
	<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
	<b>threshold-in msgs count</b>	(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.

**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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 Operating System Configuration Guide*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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).

### Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data          Mask          From To  #Covered
1 00001111110100000 11111111111100000 4000 4031 32
2 00001111111000000 11111111111100000 4032 4095 64
3 00010000000000000 11111000000000000 4096 6143 2048
4 00011000000000000 11111100000000000 6144 7167 1024
5 00011100000000000 11111110000000000 7168 7679 512
6 00011110000000000 11111111000000000 7680 7935 256
7 00011111000000000 11111111110000000 7936 7999 64
8 00011111010000000 11111111111111111 8000 8000 1

Total Ports: 4001
```

### Example

An ACL rule with a TCP port 1023 uses only one entry in the CAM.

```
Dell# Data          Mask          From To  #Covered
1 00000000000000000 11111100000000000 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.

## 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]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]]
```

### Parameters

- sequence-number*** Enter a number from 0 to 4294967290. The range is from 1 to 65534.
- deny** Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- permit** Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
- ip-protocol-number*** Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.

<b>icmp</b>	Enter the keyword <code>icmp</code> to configure an ICMP access list filter.
<b>ip</b>	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.
<b>tcp</b>	Enter the keyword <code>tcp</code> to configure a TCP access list filter.
<b>udp</b>	Enter the keyword <code>udp</code> to configure a UDP access list filter.
<b>source</b>	Enter an IP address in dotted decimal format of the network from which the packet was received.
<b>mask</b>	(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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address or hostname.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operands: <ul style="list-style-type: none"> <li>• <code>eq</code> = equal to</li> <li>• <code>neq</code> = not equal to</li> <li>• <code>gt</code> = greater than</li> <li>• <code>lt</code> = less than</li> <li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter.)</li> </ul>
<b>port port</b>	(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: <ul style="list-style-type: none"> <li>• 23 = Telnet</li> <li>• 20 and 21 = FTP</li> <li>• 25 = SMTP</li> <li>• 169 = SNMP</li> </ul>
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
<b>monitor</b>	(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 the ACL logs are generated is five minutes. By default, the flow-based monitoring is not enabled.

**Command Modes** CONFIGURATION-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for the flow-based monitoring on the MXL 10/40GbE Switch IO Module.
9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

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

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.

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

The switch supports both Ingress and Egress MAC ACLs.

# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.


## mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. Enter into the Interface mode and apply the MAC ACL in the following manner.

**Syntax** `mac access-group access-list-name {in [vlan vlan-range] | out}`

To delete a MAC access-group, use the `no mac access-group mac-list-name` command.

**Parameters**

- access-list-name** Enter the name of a configured MAC access list, up to 140 characters.
- vlan vlan-range** (OPTIONAL) Enter the keyword `vlan` and then enter a range of VLANs. The range is from 1 to 4094 (you can use IDs 1 to 4094).  
 **NOTE:** This option is available only with the keyword `in` option.
- in** Enter the keyword `in` to configure the ACL to filter incoming traffic.
- out** Enter the keyword `out` to configure the ACL to filter outgoing traffic.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can assign one ACL (standard or extended) to an interface.

In case of applying a MAC ACL to traffic entering or exiting a VLAN interface. Enter the VLAN interface mode and apply the `mac acl` in the following manner.

`mac access-group access-list-name {in | out}`

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.

**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 or number information:

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

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 or number information:

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

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

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

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

**Example**

```
Dell#show mac accounting access-list TestMac interface
tengigabitethernet 0/1 in
Ingress Standard mac access-list TestMac on TenGigabitEthernet 0/1
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.

The switch 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]]
```

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**

<b>any</b>	Enter the keyword <code>any</code> to drop all packets.
<b>host mac-address</b>	Enter the keyword <code>host</code> and then enter a MAC address to drop packets with that host address.
<b>mac-source-address</b>	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<b>mac-source-address-mask</b>	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.
<b>mac-destination-address</b>	Enter the destination MAC address and mask in <code>nn:nn:nn:nn:nn:nn</code> format.
<b>mac-destination-address-mask</b>	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.

<b><i>etherstype operator</i></b>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: <ul style="list-style-type: none"> <li>• <code>ev2</code> - is the Ethernet II frame format</li> <li>• <code>11c</code> - is the IEEE 802.3 frame format</li> <li>• <code>snap</code> - is the IEEE 802.3 SNAP frame format</li> </ul>
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.

**Defaults** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

[permit](#) — configures a MAC address filter to pass packets.

[seq](#) — configures a MAC address filter with a specified sequence number.

## 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 [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		
<b>any</b>		Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b><i>mac-source-address</i></b>		Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<b><i>mac-source-address-mask</i></b>		(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).
<b>count</b>		(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>		(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>		(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>		(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.
<b>interval minutes</b>		(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.
<b>monitor</b>		(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**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.

## mac access-list extended

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

**Syntax** `mac access-list extended access-list-name [cpu-qos]`

**Parameters**

- access-list-name*** Enter a text string as the MAC access list name, up to 140 characters.
- cpu-qos*** Enter the keyword `cpu-qos` to assign this ACL to control plane traffic only (CoPP).

**Defaults** None

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

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



## Example

```
Dell(conf)#mac-access-list access-list extended TestMATExt
Dell(config-ext-macl)#remark 5 IPv4
Dell(config-ext-macl)#seq 10 permit any any ev2 eq 800 count bytes
Dell(config-ext-macl)#remark 15 ARP
Dell(config-ext-macl)#seq 20 permit any any ev2 eq 806 count bytes
Dell(config-ext-macl)#remark 25 IPv6
Dell(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
Dell(config-ext-macl)#seq 40 permit any any count bytes
Dell(config-ext-macl)#exit
Dell(conf)#do show mac accounting access-list snickers interface g0/47 in
Extended mac access-list snickers on TenGigabitEthernet 0/12
seq 10 permit any any ev2 eq 800 count bytes (559851886 packets
191402152148bytes)seq 20 permit any any ev2 eq 806 count bytes
(74481486 packets 5031686754bytes)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 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

<b>any</b>	Enter the keyword <code>any</code> to forward all packets received with a MAC address.
<b><i>mac-source-address</i></b>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<b><i>mac-source-address-mask</i></b>	(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).
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs <i>count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-STANDARD

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

When the configured maximum threshold is exceeded, generation of logs are 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, Pv6 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

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

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

<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs count</b>	(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.
<b>interval minutes</b>	(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..
<b>monitor</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## 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 Switch supports both Ingress and Egress MAC ACLs.

# 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.

**Syntax** `mac access-list standard mac-list-name`

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The Dell operating system supports one ingress and one egress MAC ACL per interface.

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

The switch supports both ingress and egress ACLs.

**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 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]]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | mac-destination-address mac-destination-address-mask}` command.

**Parameters**

**any** Enter the keyword `any` to forward all packets.

**host** Enter the keyword `host` then a MAC address to forward packets with that host address.

**mac-source-address** Enter a MAC address in `nn:nn:nn:nn:nn:nn` format.

**mac-source-address-mask** (OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of `ff:ff:ff:ff:ff:ff` allows entries that do not match and a mask of `00:00:00:00:00:00` only allows entries that match exactly.

**mac-destination-address** Enter the destination MAC address and mask in `nn:nn:nn:nn:nn:nn` format.

<b><i>mac-destination-address-mask</i></b>	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b><i>etherstype operator</i></b>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: <ul style="list-style-type: none"> <li>• <code>ev2</code> - is the Ethernet II frame format</li> <li>• <code>11c</code> - is the IEEE 802.3 frame format</li> <li>• <code>snap</code> - is the IEEE 802.3 SNAP frame format</li> </ul>
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.

**Defaults** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

`deny` — configures a MAC ACL filter to drop packets.

`seq` — configure a MAC ACL filter with a specified sequence number.

## seq

Configure a filter with a specific sequence number.

**Syntax**

```
seq sequence-number {deny | permit} {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [etherstype operator] [count [byte]]
```

<b>Parameters</b>	<b><i>sequence-number</i></b>	Enter a number as the filter sequence number. The range is from zero (0) to 65535.
	<b>deny</b>	Enter the keyword <code>deny</code> to drop any traffic matching this filter.
	<b>permit</b>	Enter the keyword <code>permit</code> to forward any traffic matching this filter.
	<b>any</b>	Enter the keyword <code>any</code> to filter all packets.
	<b>host mac-address</b>	Enter the keyword <code>host</code> and then enter a MAC address to filter packets with that host address.
	<b>mac-source-address</b>	Enter a MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
	<b>mac-source-address-mask</b>	Specify which bits in the MAC address must be matched.
	<b>mac-destination-address</b>	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
	<b>mac-destination-address-mask</b>	Specify which bits in the MAC address must be matched.

The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

<b><i>ethertype operator</i></b>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: <ul style="list-style-type: none"><li>• <code>ev2</code> - is the Ethernet II frame format.</li><li>• <code>11c</code> - is the IEEE 802.3 frame format.</li><li>• <code>snap</code> - is the IEEE 802.3 SNAP frame format.</li></ul>
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.

**Defaults** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-STANDARD

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

## IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. To configure or enable IP prefix lists, use these commands.

### clear ip prefix-list

Reset the number of times traffic meets the conditions (“hit” counters) of the configured prefix lists.

<b>Syntax</b>	<code>clear ip prefix-list [prefix-name]</code>						
<b>Parameters</b>	<b><i>prefix-name</i></b> (OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.						
<b>Defaults</b>	Clears “hit” counters for all prefix lists unless a prefix list is specified.						
<b>Command Modes</b>	EXEC Privilege						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<a href="#">ip prefix-list</a> — configures a prefix list.						

# deny

To drop packets meeting the criteria specified, configure a filter.

<b>Syntax</b>	<code>deny ip-prefix [ge min-prefix-length] [le max-prefix-length]</code>	
<b>Parameters</b>	<b><i>ip-prefix</i></b>	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.
	<b><i>ge min-prefix-length</i></b>	(OPTIONAL) Enter the keyword <i>ge</i> and then enter the minimum prefix length, which is a number from zero (0) to 32.
	<b><i>le max-prefix-length</i></b>	(OPTIONAL) Enter the keyword <i>le</i> and then enter the maximum prefix length, which is a number from zero (0) to 32.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	PREFIX-LIST	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Sequence numbers for this filter are automatically assigned starting at sequence number 5.	
	If you do not use the <i>ge</i> or <i>le</i> options, only packets with an exact match to the prefix are filtered.	
<b>Related Commands</b>	<a href="#">permit</a> — configures a filter to pass packets.	
	<a href="#">seq</a> — configures a drop or permit filter with a specified sequence number.	

# ip prefix-list

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

<b>Syntax</b>	<code>ip prefix-list prefix-name</code>	
<b>Parameters</b>	<b><i>prefix-name</i></b>	Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Prefix lists redistribute OSPF and RIP routes meeting specific criteria.	
<b>Related Commands</b>	<a href="#">show ip route list</a> — displays IP routes in an IP prefix list.	
	<a href="#">show ip prefix-list summary</a> — displays a summary of the configured prefix lists.	

# permit

Configure a filter that passes packets meeting the criteria specified.

<b>Syntax</b>	<code>permit ip-prefix [ge min-prefix-length] [le max-prefix-length]</code>	
<b>Parameters</b>	<b><i>ip-prefix</i></b>	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.
	<b><i>ge min-prefix-length</i></b>	(OPTIONAL) Enter the keyword <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
	<b><i>le max-prefix-length</i></b>	(OPTIONAL) Enter the keyword <code>le</code> and then enter the maximum prefix length, which is a number from zero (0) to 32.
<b>Command Modes</b>	PREFIX-LIST	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Sequence numbers for this filter are automatically assigned starting at sequence number 5. If you do not use the <code>ge</code> or <code>le</code> options, only packets with an exact match to the prefix are filtered.	
<b>Related Commands</b>	<a href="#">deny</a> — configures a filter to drop packets.	
	<a href="#">seq</a> — configures a drop or permit filter with a specified sequence number.	

# seq

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

<b>Syntax</b>	<code>seq sequence-number {deny   permit} {any}   [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}]   [bitmask number]</code>	
<b>Parameters</b>	<b><i>sequence-number</i></b>	Enter a number. The range is from 1 to 4294967294.
	<b><i>deny</i></b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition..
	<b><i>permit</i></b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this condition.
	<b><i>any</i></b>	(OPTIONAL) Enter the keyword <code>any</code> to match any packets.
	<b><i>ip-prefix /nn</i></b>	(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.
	<b><i>ge min-prefix-length</i></b>	(OPTIONAL) Enter the keyword <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
	<b><i>le max-prefix-length</i></b>	(OPTIONAL) Enter the keyword <code>le</code> and then enter the maximum prefix length, which is a number from zero (0) to 32.
	<b><i>bitmask number</i></b>	Enter the keyword <code>bitmask</code> then enter a bit mask number in dotted decimal format.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	PREFIX-LIST	



**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

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

## show config

Display the current PREFIX-LIST configurations.

**Syntax** `show config`

**Command Modes** PREFIX-LIST

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `continue [sequence-number]`
- Parameters** *sequence-number* (OPTIONAL) Enter the route map sequence number. The range is from 1 to 65535. The default is: no sequence number

**Defaults** Not configured

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 metric](#) — Specifies a COMMUNITY attribute  
[set automatic-tag](#) — Configures a filter to modify the AS path

## description

Add a description to this route map.

**Syntax** `description description`

**Parameters** *description* Enter a description to identify the route map (80 characters maximum).

**Defaults** none

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [route-map](#) — Enables a route map.

## 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 or number information:

- For the Loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- For a Ten Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** Not configured.

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.0</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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`

**Parameters** ***prefix-list-name*** Enter the name of configured prefix list, up to 140 characters.

**Defaults** Not configured.

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 {access-list | prefix-list prefix-list-name}`

**Parameters** ***access-list-name*** Enter the name of a configured IP access list, up to 140 characters.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `match ip route-source {access-list | prefix-list prefix-list-name}`

**Parameters**

- access-list-name*** Enter the name of a configured IP access list, up to 140 characters.
- 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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`

**Parameters**      *metric-value*      Enter a value to match. The range is from zero (0) to 4294967295.

**Defaults**      Not configured.

**Command Modes**      ROUTE-MAP

**Supported Modes**      Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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 | local}`

**Parameters**

- external [type-1] type-2]**      Enter the keyword `external` then either `type-1` or `type-2` to match only on OSPF Type 1 routes or OSPF Type 2 routes.
- internal**      Enter the keyword `internal` to match only on routes generated within OSPF areas.
- local**      Enter the keyword `local` to match only on routes generated within the switch.

**Defaults**      Not configured.

**Command Modes**      ROUTE-MAP

**Supported Modes**      Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>match tag tag-value</code>	
<b>Parameters</b>	<b>tag-value</b>	Enter a value as the tag on which to match. The range is from zero (0) to 4294967295.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTE-MAP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">match interface</a> — redistributes routes that match the next-hop interface. <a href="#">match ip address</a> — redistributes routes that match an IP address. <a href="#">match ip next-hop</a> — redistributes routes that match the next-hop IP address. <a href="#">match ip route-source</a> — redistributes routes that match routes advertised by other routers. <a href="#">match metric</a> — redistributes routes that match a specific metric. <a href="#">match route-type</a> — 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.

<b>Syntax</b>	<code>route-map map-name [permit   deny] [sequence-number]</code>	
<b>Parameters</b>	<b>map-name</b>	Enter a text string of up to 140 characters to name the route map for easy identification.
	<b>permit</b>	(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> .
	<b>deny</b>	(OPTIONAL) Enter the keyword <code>deny</code> to set the route map default as deny.
	<b>sequence-number</b>	(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.
<b>Defaults</b>	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.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module
<b>Usage Information</b>	Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same <code>map-name</code> are deleted when you use the <code>no route-map map-name</code> command.	

## Example

```
Dell(conf)#route-map dempsey
Dell(config-route-map)#
```

## Related Commands

[show config2](#) — displays the current configuration.

# set automatic-tag

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

## Syntax

```
set automatic-tag
```

To return to the default, use the `no set automatic-tag` command.

## Defaults

Not configured.

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

## Command History

### Version

### Description

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

## Related Commands

[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 metric

To assign a new metric to redistributed routes, configure a filter.

## Syntax

```
set metric [+ | -] metric-value
```

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

## Parameters

**+**

(OPTIONAL) Enter + to add a metric-value to the redistributed routes.

**-**

(OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.

**metric-value**

Enter a number as the new metric value. The range is from zero (0) to 4294967295.

## Defaults

Not configured.

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

## Command History

### Version

### Description

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

## Related Commands

[set automatic-tag](#) — computes the tag value of the route.

[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.

<b>Syntax</b>	<code>set metric-type {internal   external   type-1   type-2}</code>	
<b>Parameters</b>	<b>internal</b>	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.
	<b>external</b>	Enter the keyword <code>external</code> to assign the IS-IS external metric.
	<b>type-1</b>	Enter the keyword <code>type-1</code> to assign the OSPF Type 1 metric.
	<b>type-2</b>	Enter the keyword <code>type-2</code> to assign the OSPF Type 2 metric.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTE-MAP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">set automatic-tag</a> — computes the tag value of the route.	
	<a href="#">set metric</a> — specifies the metric value assigned to redistributed routes.	
	<a href="#">set tag</a> — specifies the tag assigned to redistributed routes.	

# set tag

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

<b>Syntax</b>	<code>set tag tag-value</code>	
<b>Parameters</b>	<b>tag-value</b>	Enter a number as the tag. The range is from zero (0) to 4294967295.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTE-MAP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">set automatic-tag</a> — computes the tag value of the route.	
	<a href="#">set metric</a> — specifies the metric value assigned to redistributed routes.	
	<a href="#">set metric-type</a> — specifies the route type assigned to redistributed routes.	

# show config

Display the current route map configuration.

<b>Syntax</b>	<code>show config</code>
---------------	--------------------------

**Command Modes** ROUTE-MAP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on MXL 10/40GbE Switch IO Module

**Example**

```
Dell(config-route-map)#show config
!
route-map hopper permit 10
Dell(config-route-map)#
```

## show route-map

Display the current route map configurations.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

**source** Enter the IP address of the network or host from which the packets were sent.

**any** Enter the keyword any to specify that all routes are subject to the filter.

**host *ip-address*** Enter the keyword host then the IP address to specify a host IP address.

<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>order</b>	(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).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs <i>count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the 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).

**Related Commands**

- [ip access-list standard](#) — configures a standard ACL.
- [permit](#) — configures a permit filter.

# deny

To drop packets with a certain IP address, 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		
<b>source</b>		Enter the IP address in dotted decimal format of the network from which the packet was sent.
<b>mask</b>	(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 (discontiguous).
<b>any</b>		Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host <i>ip-address</i></b>		Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address only.
<b>count</b>	(OPTIONAL)	Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL)	Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL)	Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in <i>msgs count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
	<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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 s 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 the specified traffic instead of 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 MAC address filter to pass packets.

`seq` — configures a MAC address filter with a specified sequence number.

## 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} {source [mask] | any | host ip-address}} [count [byte] [dscp value] [order] [fragments] [threshold-in-msgs [count]]
```

### Parameters

<b>sequence-number</b>	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
<b>deny</b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
<b>permit</b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
<b>source</b>	Enter an IP address in dotted decimal format of the network from which the packet was received.
<b>mask</b>	(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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).

<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.

**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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

When 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` — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

# 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] [threshold-in-msgs [count]]`

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

<b>source</b>	Enter the IP address of the network or host from which the packets are sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>bit</b>	Enter a flag or combination of bits: <ul style="list-style-type: none"><li>• <code>ack</code>: acknowledgement field</li><li>• <code>fin</code>: finish (no more data from the user)</li><li>• <code>psh</code>: push function</li><li>• <code>rst</code>: reset the connection</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>urg</code>: urgent field</li></ul>
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li></ul>
<b>port port</b>	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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li><li>• 169 = SNMP</li></ul>
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

**threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

**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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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).

**Example** An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Dell#	Data	Mask	From	To	#Covered
1	00001111110100000	11111111111100000	4000	4031	32
2	00001111111000000	11111111111000000	4032	4095	64
3	00010000000000000	11111000000000000	4096	6143	2048
4	00011000000000000	11111100000000000	6144	7167	1024
5	00011100000000000	11111110000000000	7168	7679	512
6	00011110000000000	11111111000000000	7680	7935	256
7	00011111000000000	11111111110000000	7936	7999	64
8	00011111010000000	11111111111111111	8000	8000	1



```
Total Ports: 4001
```

### Example

An ACL rule with a TCP port 1023 uses only one entry in the CAM.

```
Dell# 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] [threshold-in-msgs [count]]
```

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li></ul>
<b>port port</b>	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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 ( <b>255</b> ).

**fragments** Enter the keyword `fragments` to use ACLs to control packet fragments.

**threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword then a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs are terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

**Defaults** By default 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which the ACL logs are generated is five minutes.

**Command Modes** CONFIGURATION-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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

**Example** An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```

Dell# 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 0001111110100000 1111111111111111 8000 8000 1

Total Ports: 4001

```

**Example** An ACL rule with a TCP port `lt 1023` uses only one entry in the CAM.

```

Dell# 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.

# 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

<b>destination-mac-address mac-address-mask</b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b>any</b>	Enter the keyword <code>any</code> to match and drop any ARP traffic on the interface.  <code>vlan vlan-id</code> Enter the keyword <code>vlan</code> and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale ( you can use IDs 1 to 4094). To filter all VLAN traffic, specify VLAN 1.  <code>ip-address</code> Enter an <i>IP address</i> in dotted decimal format (A.B.C.D) as the target IP address of the ARP.  <code>opcode code-number</code> Enter the keyword <code>opcode</code> and then enter the number of the ARP opcode. The range is from 1 to 23.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>order</b>	(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).
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platforms.
	<b>8.2.1.0</b>	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
	<b>8.1.1.0</b>	Introduced on the E-Series ExaScale.
	<b>7.4.1.0</b>	Added the support for the non-contiguous mask and the monitor option.
	<b>6.5.1.0</b>	Expanded to include the optional QoS order priority for the ACL entry.

### 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).

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](#).

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

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs (ARP and Ether-type) to Layer 2 interfaces only.

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

## 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][threshold-in-msgs] [count]]
```

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>dscp</b>	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.

## 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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
<b>9.3(0.0)</b>	Added the support for logging ACLs on the MXL 10/40GbE Switch IO Module.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 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 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

<b>protocol-type-number</b>	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
<b>destination-mac-address mac-address-mask</b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b>any</b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
<b>vlan vlan-id</b>	Enter the keyword <code>vlan</code> and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale ( you can use IDs 1 to 4094). To filter all VLAN traffic, specify <code>VLAN 1</code> .
<b>source-mac-address mac-address-mask</b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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).
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.

<b>interval <i>minutes</i></b>	(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 of 1 to 10 minutes.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the 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 `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

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.

<b>Parameters</b>		
<b>any</b>		Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>mac-source-address</b>		Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<b>mac-source-address-mask</b>	(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).

<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs <i>count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**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

To drop packets with a certain IP address, 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}`



```
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

<b>source</b>	Enter the IP address in dotted decimal format of the network from which the packet was sent.
<b>mask</b>	(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 (discontiguous).
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address only.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module.
<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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*.

You can configure either `count` (packets) or `count` (bytes). However, for an ACL with multiple rules, you can configure some ACLs with `count` (packets) and others as `count` (bytes) at any given time.

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 s 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 the specified traffic instead of 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 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} [no-drop] [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

<b>source</b>	Enter the IP address in dotted decimal format of the network from which the packet was sent.
<b>mask</b>	(OPTIONAL) Enter a network <code>mask</code> 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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
<b>no-drop</b>	Enter the keywords <code>no-drop</code> to match only the forwarded packets.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>bytes</b>	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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 *minutes*** (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

**monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults** By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes** CONFIGURATION-STANDARD-ACCESS-LIST

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added support for logging of ACLs on the 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).

**Related Commands**

`deny` — assigns a IP ACL filter to deny IP packets.

`ip access-list standard` — creates a standard ACL.

## 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 [interval minutes] [threshold-in-msgs[count] [monitor]]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

**Parameters**

**any** Enter the keyword `any` to forward all packets received with a MAC address.

<b><i>mac-source-address</i></b>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<b><i>mac-source-address-mask</i></b>	(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).
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-STANDARD

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs are 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, Pv6 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.

# 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 [intervalminutes][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

<b>protocol-type-number</b>	Enter a number from 600 to FFF as the specific Ethernet type traffic to drop.
<b>destination-mac-address mac-address-mask</b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b>any</b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
<b>vlan vlan-id</b>	Enter the keyword <code>vlan</code> and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify <code>VLAN 1</code> .
<b>source-mac-address mac-address-mask</b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>interval minutes</b>	(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.
<b>threshold-in msgs count</b>	(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.
<b>monitor</b>	(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** 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.2.1.0</b>	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
	<b>8.1.1.0</b>	Introduced on the E-Series ExaScale.
	<b>7.4.1.0</b>	Added the <code>monitor</code> option.
	<b>6.5.10</b>	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*.

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

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.

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

You cannot include IP, TCP, or UDP filters in an ACL configured with ARP filters.

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

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] [threshold-in-msgs [count]]`

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is 0 to 63.
<b>message-type</b>	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.

## 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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 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

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] [threshold-in-msgs [count]]`

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter)</li></ul>
<b>port port</b>	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.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in-msgs count</b>	(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.

**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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 Operating System Configuration Guide*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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).

**Example** An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

Dell#	Data	Mask	From	To	#Covered
1	00001111110100000	11111111111100000	4000	4031	32
2	00001111111000000	11111111111000000	4032	4095	64
3	00010000000000000	11111000000000000	4096	6143	2048
4	00011000000000000	11111100000000000	6144	7167	1024
5	00011100000000000	11111110000000000	7168	7679	512
6	00011110000000000	11111111000000000	7680	7935	256
7	00011111000000000	11111111100000000	7936	7999	64
8	00011111101000000	11111111111111111	8000	8000	1
Total Ports: 4001					

**Example** An ACL rule with a TCP port `lt 1023` uses only one entry in the CAM.

Dell#	Data	Mask	From	To	#Covered
1	00000000000000000	11111100000000000	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.

# 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

<b>source</b>	Enter the IP address in dotted decimal format of the network from which the packet was sent.
<b>mask</b>	(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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>bytes</b>	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DCSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

## 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 tcp](#) — assigns a permit filter for TCP packets.
- [permit udp](#) — assigns a permit filter for UDP packets.

# 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 [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

<b>any</b>	Enter the keyword <code>any</code> to forward all packets received with a MAC address.
<b>mac-source-address</b>	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<b>mac-source-address-mask</b>	(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).
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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 *minutes*** (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

**monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface

**Defaults** Not configured.

**Command Modes** CONFIGURATION-MAC ACCESS LIST-STANDARD

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
9.3(0.0)	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs are 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, Pv6 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

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**

***sequence-number*** Enter a number from 0 to 65535.

<b>deny</b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
<b>permit</b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
<b>any</b>	Enter the keyword <code>any</code> to filter all packets.
<b>mac-source-address</b>	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<b>mac-source-address-mask</b>	(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).
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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..
<b>monitor</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>bit</b>	Enter a flag or combination of bits: <ul style="list-style-type: none"><li>• <code>ack</code>: acknowledgement field</li><li>• <code>fin</code>: finish (no more data from the user)</li><li>• <code>psh</code>: push function</li><li>• <code>rst</code>: reset the connection</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>urg</code>: urgent field</li></ul>
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the port parameter)</li></ul>
<b>port port</b>	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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li><li>• 169 = SNMP</li></ul>
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.

<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs <i>count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

#### 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 switch cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

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.

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).

### Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```

Dell# Data                Mask                From To  #Covered
1 00001111110100000 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 1023 uses only one entry in the CAM.

```

Dell# 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.

## seq arp

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.

### 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

- sequence-number*** Enter a number from 0 to 4294967290.
- deny** Enter the keyword `deny` to drop all traffic meeting the filter criteria..
- permit** Enter the keyword `permit` to forward all traffic meeting the filter criteria.
- destination-mac-address mac-address-mask*** Enter a MAC address and mask in the `nn:nn:nn:nn:nn` format.  
For the MAC address mask, specify which bits in the MAC address must match.  
The MAC ACL supports an inverse mask; therefore, a mask of `ff:ff:ff:ff:ff` allows entries that do not match and a mask of `00:00:00:00:00:00` only allows entries that match exactly.
- any** Enter the keyword `any` to match and drop any ARP traffic on the interface.



<b>vlan <i>vlan-id</i></b>	Enter the keyword <code>vlan</code> followed by the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify <code>VLAN 1</code> .
<b>ip-address</b>	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
<b>opcode <i>code-number</i></b>	Enter the keyword <code>opcode</code> and then enter the number of the ARP opcode. The range is 1 to 16.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>interval <i>minutes</i></b>	(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.
<b>threshold-in msgs <i>count</i></b>	(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.
<b>monitor</b>	(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

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

**Supported Modes** Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.2.1.0</b>	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
<b>8.1.1.0</b>	Introduced on the E-Series ExaScale.
<b>7.4.1.0</b>	Added the <code>monitor</code> option.
<b>6.5.10</b>	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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.

- If *sequence-number* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *sequence-number* is configured, the sequence-number is used as a tie breaker for rules with the same order.


When you use the `log` option, the CP processor logs 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.

You cannot include IP, TCP, or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.

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).

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

## seq ether-type

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.


### 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

<b><i>sequence-number</i></b>	Enter a number from 0 to 4294967290.
<b><i>deny</i></b>	Enter the keyword <code>deny</code> to drop all traffic meeting the filter criteria..
<b><i>permit</i></b>	Enter the keyword <code>permit</code> to forward all traffic meeting the filter criteria.
<b><i>destination-mac-address mac-address-mask</i></b>	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
<b><i>any</i></b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.

<b>vlan <i>vlan-id</i></b>	Enter the keyword <code>vlan</code> and then enter the VLAN ID to filter traffic associated with a specific VLAN. The range is 1 to 4094 and 1 to 2094 for ExaScale (you can use IDs 1 to 4094). To filter all VLAN traffic specify <code>VLAN 1</code> .
<b><i>source-mac-address mac-address-mask</i></b>	Enter a MAC address and mask in the <code>nn:nn:nn:nn:nn</code> format. For the MAC address mask, 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</code> allows entries that do not match and a mask of <code>00:00:00:00:00</code> only allows entries that match exactly.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default (255).
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>interval <i>minutes</i></b>	(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.
<b>threshold-in-msgs <i>count</i></b>	(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.
<b>monitor</b>	(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.  <b>NOTE:</b> 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** 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.2.1.0</b>	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
	<b>8.1.1.0</b>	Introduced on the E-Series ExaScale.
	<b>7.4.1.0</b>	Added the <code>monitor</code> option.
	<b>6.5.10</b>	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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.


When you use the `log` option, the CP processor logs 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.

You cannot include IP, TCP, or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.

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).

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

## seq

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

<b>Syntax</b>	<code>seq sequence-number {deny   permit} {source [mask]   any   host ip-address}} [count [byte] [dscp value] [order] [fragments] [threshold-in-msgs [count]]</code>	
<b>Parameters</b>	<b><i>sequence-number</i></b>	Enter a number from 0 to 4294967290. The range is from 0 to 65534.
	<b><i>deny</i></b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
	<b><i>permit</i></b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
	<b><i>source</i></b>	Enter an IP address in dotted decimal format of the network from which the packet was received.
	<b><i>mask</i></b>	(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.
	<b><i>any</i></b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	<b><i>count</i></b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
	<b><i>byte</i></b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.

<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in msgs count</b>	(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.

**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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

When 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` — assigns a sequence number to a deny or permit filter in an IP access list while creating the filter.

# 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} {ipv6-protocol-number | icmp | ip | tcp | udp} {source mask | any | host ipv6-address} {destination mask | any | host ipv6-address} [operator port [port]] [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

<b>Parameters</b>	<b>sequence-number</b>	Enter a number from 0 to 4294967290. The range is from 1 to 65534.
	<b>deny</b>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
	<b>permit</b>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
	<b>ipv6-protocol-number</b>	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
	<b>icmp</b>	Enter the keyword <code>icmp</code> to configure an ICMP access list filter.
	<b>ip</b>	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.
	<b>tcp</b>	Enter the keyword <code>tcp</code> to configure a TCP access list filter.
	<b>udp</b>	Enter the keyword <code>udp</code> to configure a UDP access list filter.
	<b>source</b>	Enter an IP address in dotted decimal format of the network from which the packet was received.
	<b>mask</b>	(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.
	<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	<b>host ipv6-address</b>	Enter the keyword <code>host</code> and then enter the IPv6 address to specify a host IP address or hostname.
	<b>operator</b>	(OPTIONAL) Enter one of the following logical operands: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter.)</li></ul>
	<b>port port</b>	(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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li><li>• 169 = SNMP</li></ul>
	<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
	<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
	<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
	<b>order</b>	(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 `order`, the ACLs have the lowest order by default (**255**).

<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b><i>threshold-in msgs count</i></b>	(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.
<b><i>interval minutes</i></b>	(OPTIONAL) Enter the keyword <code>interval</code> followed by the time period in minutes at which the ACL logs must be generated. The interval range is from 1 to 10 minutes.
<b>monitor</b>	(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 the ACL logs are generated is five minutes. By default, the flow-based monitoring is not enabled.

**Command Modes** ACCESS-LIST

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for the flow-based monitoring on the MXL 10/40GbE Switch IO Module.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If `sequence-number` is not configured, the rules with the same order value are ordered according to their configuration order.
- If `sequence-number` is configured, the sequence-number is used as a tie breaker for rules with the same order.

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

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 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] [threshold-in-msgs [count]]
```

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter)</li></ul>
<b>port port</b>	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.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>threshold-in-msgs count</b>	(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.

## 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-IP ACCESS-LIST-EXTENDED



**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 Operating System Configuration Guide*.

You can configure either count (packets) or count (bytes). However, for an ACL with multiple rules, you can configure some ACLs with count (packets) and others as count (bytes) at any given time.

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.

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).

**Example**

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Dell# Data Mask From To #Covered
1 00001111110100000 11111111111100000 4000 4031 32
2 00001111111000000 11111111111000000 4032 4095 64
3 00010000000000000 11111000000000000 4096 6143 2048
4 00011000000000000 11111100000000000 6144 7167 1024
5 00011100000000000 11111110000000000 7168 7679 512
6 00011110000000000 11111111000000000 7680 7935 256
7 00011111000000000 11111111100000000 7936 7999 64
8 00011111010000000 11111111111111111 8000 8000 1

Total Ports: 4001
```

**Example**

An ACL rule with a TCP port `lt 1023` uses only one entry in the CAM.

```
Dell# Data Mask From To #Covered
1 00000000000000000 11111100000000000 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.

# 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][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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>bit</b>	Enter a flag or combination of bits: <ul style="list-style-type: none"><li>• <code>ack</code>: acknowledgement field</li><li>• <code>fin</code>: finish (no more data from the user)</li><li>• <code>psh</code>: push function</li><li>• <code>rst</code>: reset the connection</li><li>• <code>syn</code>: synchronize sequence numbers</li><li>• <code>urg</code>: urgent field</li></ul>
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li><li>• <code>range</code> = inclusive range of ports (you must specify two ports for the port parameter)</li></ul>
<b>port port</b>	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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li><li>• 169 = SNMP</li></ul>
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>mask</b>	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.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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-IP ACCESS-LIST-EXTENDED

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**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 switch cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

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.

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).

**Example**

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```

Dell# Data                Mask                From To  #Covered
-----
1 0000111110100000 1111111111100000 4000 4031 32

```

```

2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111110000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001

```

### Example

An ACL rule with a TCP port 1023 uses only one entry in the CAM.

```

Dell# 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 icmp

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]
[threshold-in-msgs [count]]

```

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

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to match and drop specific Ethernet traffic on the interface.
<b>host ip-address</b>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>dscp</b>	Enter the keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is 0 to 63.
<b>message-type</b>	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is 0 to 255 for ICMP type and 0 to 255 for ICMP code.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword <code>order</code> , the ACLs have the lowest order by default ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.

**threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

**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-IP ACCESS-LIST-STANDARD

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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

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]`

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**

<b>ip-protocol-number</b>	Enter an IPv6 protocol number. The range is from 0 to 255.
<b>icmp</b>	Enter the keyword <code>icmp</code> to filter internet Control Message Protocol version 6.
<b>ipv6</b>	Enter the keyword <code>ipv6</code> to filter any internet Protocol version 6.

<b>tcp</b>	Enter the keyword <code>tcp</code> to filter the Transmission Control protocol.
<b>udp</b>	Enter the keyword <code>udp</code> to filter the User Datagram Protocol.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(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 ( <b>255</b> ).
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs</b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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** Not configured.

**Command Modes** ACCESS-LIST

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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		
<b>source</b>	Enter the IP address of the network or host from which the packets are sent.	
<b>mask</b>	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.	
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.	

<b>host <i>ipv6-address</i></b>	Enter the keyword <code>host</code> then the IPv6 address to specify a host IP address.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand. <ul style="list-style-type: none"> <li>• <code>eq</code> = equal to</li> <li>• <code>neq</code> = not equal to</li> <li>• <code>gt</code> = greater than</li> <li>• <code>lt</code> = less than</li> <li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li> </ul>
<b>port</b>	Enter the application layer port number. Enter two port numbers if using the <code>range</code> logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: <ul style="list-style-type: none"> <li>• 23 = Telnet</li> <li>• 20 and 21 = FTP</li> <li>• 25 = SMTP</li> <li>• 169 = SNMP</li> </ul>
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count the packets that filter the processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count the bytes that filter the processes.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs <i>count</i></b>	(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.
<b>interval <i>minutes</i></b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

**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 tcp` – assigns a deny filter for TCP traffic.

## 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

<b>source</b>	Enter the IP address of the network or host from which the packets are sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ipv6-address</b>	Enter the keyword <code>host</code> then the IPv6 address to specify a host IP address.
<b>operator</b>	(OPTIONAL) Enter one of the following logical operand: <ul style="list-style-type: none"><li>• eq = equal to</li><li>• neq = not equal to</li><li>• gt = greater than</li><li>• lt = less than</li><li>• range = inclusive range of ports (you must specify two ports for the <code>port</code> command)</li></ul>
<b>port</b>	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: <ul style="list-style-type: none"><li>• 23 = Telnet</li><li>• 20 and 21 = FTP</li><li>• 25 = SMTP</li></ul>



- 169 = SNMP

<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>bit</b>	(OPTIONAL) Enter the keyword <code>bit</code> to count the bits that filter the processes.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count the packets that filter the processes.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count the bytes that filter the processes.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Added support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

#### 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 icmp (for Extended IPv6 ACLs)

Configure a filter to drop all or specific ICMP messages.

**Syntax** `deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [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

<b>source</b>	Enter the IPv6 address of the network or host from which the packets were sent.
<b>mask</b>	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.
<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
<b>host ipv6-address</b>	Enter the keyword <code>host</code> then the IPv6 address to specify a host IP address.
<b>destination</b>	Enter the IPv6 address of the network or host to which the packets are sent.
<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
	<b>9.3(0.0)</b>	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

**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]`

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

<b>count</b>	OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
<b>order</b>	(OPTIONAL) Enter the keyword <code>order</code> to specify the QoS order of 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 <code>order</code> keyword, the ACLs have the lowest order by default as <b>255</b> .
<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<b>threshold-in-msgs count</b>	(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.
<b>interval minutes</b>	(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.
<b>monitor</b>	(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

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform.
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform.

### 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 directions. 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).

# Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM)

This section describes the access control list (ACL) virtual local area network (VLAN) group, and content addressable memory (CAM) enhancements.

## Topics:

- [member vlan](#)
- [ip access-group](#)
- [show acl-vlan-group](#)
- [show cam-acl-vlan](#)
- [cam-acl-vlan](#)
- [show cam-usage](#)
- [show running config acl-vlan-group](#)
- [acl-vlan-group](#)
- [show acl-vlan-group detail](#)
- [description \(ACL VLAN Group\)](#)

## member vlan

Add VLAN members to an ACL VLAN group.

**Syntax** `member vlan {VLAN-range}`

**Parameters** *VLAN-range* Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example:

Comma-separated: 3, 4, 6

Range: 5-10

Combination: 3, 4, 5-10, 8

**Default** None

**Command Modes** CONFIGURATION (conf-acl-vl-grp)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**Usage Information** At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one group at any given time.

You can create an ACL VLAN group and attach the ACL with the VLAN members. The optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL has a mapping with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

# ip access-group


Apply an egress IP ACL to the ACL VLAN group.

<b>Syntax</b>	<code>ip access-group {group name} out implicit-permit</code>	
<b>Parameters</b>	<b>group-name</b>	Enter the name of the ACL VLAN group where you want the egress IP ACLs applied, up to 140 characters.
	<b>out</b>	Enter the keyword <code>out</code> to apply the ACL to outgoing traffic.
	<b>implicit-permit</b>	Enter the keyword <code>implicit-permit</code> to change the default action of the ACL from <code>implicit-deny</code> to <code>implicit-permit</code> (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
<b>Default</b>	None	
<b>Command Modes</b>	CONFIGURATION (conf-acl-vl-grp)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.
<b>Usage Information</b>	You can apply only an egress IP ACL on an ACL VLAN group.	

# show acl-vlan-group

Display all the ACL VLAN groups or display a specific ACL VLAN group, identified by name.

<b>Syntax</b>	<code>show acl-vlan-group {group-name   detail}</code>	
<b>Parameters</b>	<b>group-name</b>	(Optional) Display only the ACL VLAN group that is specified, up to 140 characters.
	<b>detail</b>	Display information in a line-by-line format to display the names in their entirety. Without the detail option, the output displays in a table style and information may be truncated.
<b>Default</b>	No default behavior or values	
<b>Command Modes</b>	EXEC	
	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.
<b>Usage Information</b>	When an ACL-VLAN-Group name or the Access List Group Name contains more than 30 characters, the name is truncated in the <code>show acl-vlan-group</code> command output.	
<b>Examples</b>	The following sample illustrates the output of the <code>show acl-vlan-group</code> command.	

 **NOTE:** Some group names and some access list names are truncated.

```
Dell#show running-config acl-vlan-group
!
```

```

acl-vlan-group Test
  member vlan 1-100
  ip access-group test in
Dell#show acl-vlan-group
Group Name      Ingress V6 Acl      Egress IP Acl      Ingress IP Acl
Test            -                    -                    test
                -                    1-100

```

The following sample output is displayed when using the `show acl-vlan-group group-name` option.

**NOTE:** The access list name is truncated.

```

Dell#show acl-vlan-group TestGroupSeventeenTwenty
Group Name      Ingress IPV6 Acl      Egress IP Acl      Ingress IP Acl
Test            -                    -                    test
                -                    1-100
Dell#

```

The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option.

**NOTE:** No group or access list names are truncated

```

Dell#show acl-vlan-group detail

Group Name :
  Test
Egress IP Acl :
  -
Ingress IP Acl :
  test
Ingress IPV6 Acl :
  -
Vlan Members :
  1-100

```

## show cam-acl-vlan

Display the number of flow processor (FP) blocks that is allocated for the different VLAN services.

**Syntax** `show cam-acl-vlan`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

**Version**

**9.9(0.0)**

**9.3(0.0)**

**Description**

Introduced on the FN IOM.

Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information**

After CAM configuration for ACL VLAN groups is performed, you must reboot the system to enable the settings to be stored in nonvolatile storage. During the initialization of CAM, the chassis manager reads the NVRAM and allocates the dynamic VCAP regions.

The following table describes the output fields of this `show` command:

**Field**

**Description**

**Chassis Vlan Cam ACL**

Details about the CAM blocks allocated for ACLs for various VLAN operations at a system-wide, global level.

Field	Description
<b>Stack Unit &lt;number&gt;</b>	Details about the CAM blocks allocated for ACLs for various VLAN operations for a particular stack unit.
<b>Current Settings(in block sizes)</b>	Information about the number of FP blocks that are currently in use or allocated.
<b>VlanOpenFlow</b>	Number of FP blocks for VLAN open flow operations.
<b>VlanIscsi</b>	Number of FP blocks for VLAN internet small computer system interface (iSCSI) counters.
<b>VlanHp</b>	Number of FP blocks for VLAN high performance processes.
<b>VlanFcoe</b>	Number of FP blocks for VLAN Fiber Channel over Ethernet (FCoE) operations.
<b>VlanAclOpt</b>	Number of FP blocks for ACL VLAN optimization feature.

### Example

```
Dell#show cam-acl-vlan

-- Chassis Vlan Cam ACL --
      Current Settings(in block sizes)
VlanOpenFlow :      0
VlanIscsi    :      0
VlanAclOpt   :      2
VlanHp       :      1
VlanFcoe     :      1
```

## cam-acl-vlan

Allocate the number of flow processor (FP) blocks or entries for VLAN services and processes.

**Syntax** `cam-acl-vlan { default | vlanopenflow <0-2> | vlaniscsi <0-2> | vlnaclopt <0-2>`

Parameters	default	Description
	<b>default</b>	Reset the number of FP blocks to default. By default, 0 groups are allocated for the ACL in VCAP. ACL VLAN groups or CAM optimization is not enabled by default, and you need to allocate the slices for CAM optimization.
	<b>vlanopenflow &lt;0-2&gt;</b>	Allocate the number of FP blocks for VLAN open flow operations.
	<b>vlaniscsi &lt;0-2&gt;</b>	Allocate the number of FP blocks for VLAN iSCSI counters.
	<b>vlnaclopt &lt;0-2&gt;</b>	Allocate the number of FP blocks for the ACL VLAN optimization feature.

**Default** If you use the `default` keyword with the `cam-acl-vlan` command, the FP blocks allocated for VLAN processes are restored to their default values. No FP blocks or dynamic VLAN Content Aware Processor (VCAP) groups are allocated for VLAN operations by default.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**Usage Information** The VLAN ContentAware Processor (VCAP) application is a pre-ingress CAP that modifies the VLAN settings before packets are forwarded. To support the ACL CAM optimization functionality, the CAM carving feature is enhanced. A total of four VACP groups are present, of which two are for fixed groups and the other two are for dynamic groups. Out of the total of two dynamic groups, you can allocate zero,



one, or two flow processor (FP) blocks to iSCSI Counters, OpenFlow and ACL Optimization. You can configure only two of these features at a point in time.

## show cam-usage

View the amount of CAM space available, used, and remaining in each partition (including IPv4Flow and Layer 2 ACL sub-partitions).

**Syntax** `show cam-usage [acl | router | switch]`

**Parameters**

- acl** (OPTIONAL) Enter the keyword `acl` to display Layer 2 and Layer 3 ACL CAM usage.
- router** (OPTIONAL) Enter the keyword `router` to display Layer 3 CAM usage.
- switch** (OPTIONAL) Enter the keyword `switch` to display Layer 2 CAM usage.

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.11.0.0</b>	The <code>show cam-usage</code> command is updated to display the ECMP group count information.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information** The following regions must be provided in the `show cam-usage` output:

- L3AcICam
- L2AcICam
- V6AcICam

The following describes the output fields of this `show` command:

Field	Description
<b>LineCard</b>	Number of the line card that contains information on ACL VLAN groups
<b>Portpipe</b>	The hardware path that packets follow through a system for ACL optimization
<b>CAM-Region</b>	Type of area in the CAM block that is used for ACL VLAN groups
<b>Total CAM space</b>	Total amount of space in the CAM block
<b>Used CAM</b>	Amount of CAM space that is currently in use
<b>Available CAM</b>	Amount of CAM space that is free and remaining to be allocated for ACLs

**Example:**

```
Dell#show cam-usage
Stackunit|Portpipe|CAM Partition |Total CAM|Used CAM|AvailableCAM
=====|=====|=====|=====|=====|=====
      0 |      0 | IN-L3 ACL | 512 | 1 | 511
      |      | IN-L3 ECMP GRP | 1024 | 0 | 1024
      |      | IN-V6 ACL | 0 | 0 | 0
      |      | IN-L2 ACL | 512 | 0 | 512
      |      | IN-NLB ACL | 256 | 0 | 256
      |      | IPMAC ACL | 0 | 0 | 0
      |      | OUT-L3 ACL | 158 | 6 | 152
      |      | OUT-V6 ACL | 158 | 1 | 157
      1 |      0 | IN-L3 ACL | 512 | 1 | 511
      |      | IN-V6 ACL | 0 | 0 | 0
```

```

|          | IN-L2 ACL      | 512    | 0    | 512
|          | IN-NLB ACL    | 256    | 0    | 256
|          | IPMAC ACL     | 0       | 0    | 0
|          | OUT-L3 ACL    | 158    | 6    | 152
|          | OUT-V6 ACL    | 158    | 1    | 157
Codes: * - cam usage is above 90%.
Dell#

```

### Example (show cam-usage router)

```

Dell#show cam-usage router
Stackunit|Portpipe| CAM Partition  | Total CAM  | Used CAM  |
Available CAM
=====|=====|=====|=====|=====|
0       | 0
| IN-L3 ACL      | 1024    | 1    | 1023
| |
| IN-L3 ECMP GRP | 1024    | 0    | 1024
| |
| IN-V6 ACL      | 0       | 0    | 0
| |
| IN-L3-MIRR ACL | 0       | 0    | 0
| |
| IN-L3 FIB      | 163840  | 15   | 163825

```

## show running config acl-vlan-group

Display the running configuration of all or a given ACL VLAN group.

**Syntax** `show running config acl-vlan-group group name`

**Parameters** *group-name* Display only the ACL VLAN group that is specified. The maximum group name is 140 characters.

**Default** None

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Examples** The following sample output shows the line-by-line style display when using the `show running-config acl-vlan-group` option. Note that no group or access list names are truncated

```

Dell#show running-config acl-vlan-group
!
acl-vlan-group Test
 member vlan 1-100
 ip access-group test in

Dell#show running-config acl-vlan-group Test
!
acl-vlan-group Test
 member vlan 1-100
 ip access-group test in

```

# acl-vlan-group

Create an ACL VLAN group.

**Syntax** `acl-vlan-group {group name}`  
To remove an ACL VLAN group, use the `no acl-vlan-group {group name}` command.

**Parameters** **group-name** Specify the name of the ACL VLAN group. The name can contain a maximum 140 characters.

**Default** No default behavior or values

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information** You can have up to eight different ACL VLAN groups at any given time. When you configure an ACL VLAN group, you enter the ACL VLAN Group Configuration mode.

To avoid the problem of excessive consumption of CAM area, you can configure ACL VLAN groups that combines all the VLANs that are applied with the same ACL in a single group. A unique identifier for each of ACL attached to the VLAN is used as a handle or locator in the CAM area instead of the VLAN id. This method of processing significantly reduces the number of entries in the CAM area and saves memory space in CAM.

You can create an ACL VLAN group and attach the ACL with the VLAN members. Optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL maps with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

# show acl-vlan-group detail

Display all the ACL VLAN Groups or display a specific ACL VLAN Group by name. To display the names in their entirety, the output displays in a line-by-line format.

**Syntax** `show acl-vlan-group detail`

**Parameters** **detail** Display information in a line-by-line format to display the names in their entirety. Without the detail option, the output is displayed in a table style and information may be truncated.

**Default** No default behavior or values

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information**

The output for this command displays in a line-by-line format. This allows the ACL-VLAN-Group names (or the Access List Group Names) to display in their entirety.

**Examples**

The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option. Note that no group or access list names are truncated

```
Dell#show acl-vlan-group detail

Group Name :
  Test
Egress IP Acl :
  -
Ingress IP Acl :
  test
Ingress IPV6 Acl :
  -
Vlan Members :
  1-100
```

## description (ACL VLAN Group)

Add a description to the ACL VLAN group.

**Syntax** `description description`

**Parameters** ***description*** Enter a description to identify the ACL VLAN group (80 characters maximum).

**Default** No default behavior or values

**Command Modes** CONFIGURATION (conf-acl-vl-grp)

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information**

Enter a description for each ACL VLAN group that you create for effective and streamlined administrative and logging purposes.

# Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.

The Dell Networking Operating System (OS) 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 virtual local area network (VLAN) interfaces and port-channels.

## Topics:

- [bfd all-neighbors](#)
- [bfd disable](#)
- [bfd enable \(Configuration\)](#)
- [bfd enable \(Interface\)](#)
- [bfd interval](#)
- [bfd protocol-liveness](#)
- [ip route bfd](#)
- [ip ospf bfd all-neighbors](#)
- [ipv6 ospf bfd all-neighbors](#)
- [isis bfd all-neighbors](#)
- [neighbor bfd](#)
- [neighbor bfd disable](#)
- [show bfd neighbors](#)
- [vrrp bfd neighbor](#)

## 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.

<b>Syntax</b>	<code>bfd all-neighbors [interval interval min_rx min_rx multiplier value role {active   passive}]</code>	
<b>Parameters</b>	<b>interval milliseconds</b>	(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 <b>200</b> . Dell EMC recommends using more than 100 milliseconds.
	<b>min_rx milliseconds</b>	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 1000. The default is <b>200</b> . Dell EMC recommends using more than 100 milliseconds.
	<b>multiplier value</b>	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 <b>3</b> .
	<b>role [active   passive]</b>	Enter the role that the local system assumes: <ul style="list-style-type: none"> <li>• <code>Active</code> — The active system initiates the BFD session. Both systems can be active for the same session.</li> <li>• <code>Passive</code> — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.</li> </ul> The default is <b>active</b> .
<b>Defaults</b>	See <i>Parameters</i> .	

**Command Modes** ROUTER OSPF  
ROUTER OSPFv3  
ROUTER BGP  
ROUTER ISIS

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

<b>Version</b>	<b>Description</b>
<b>9.13(0.0)</b>	Introduced support for enabling BFD on non-default VRFs for IPv4 BGP, default, and non-default VRFs for IPv6 BGP on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, C9010, Z9500, and Z9100-ON.
<b>9.11(2.1P1)</b>	Introduced support for enabling BFD on non-default VRFs for OSPFv2 on all the remaining Dell EMC Networking OS platforms.  Introduced support for enabling BFD on non-default VRFs for OSPFv3 on all the Dell EMC Networking OS platforms.
<b>9.10(0.2)</b>	Introduced support for enabling BFD on non-default VRFs for OSPFv2 on the S3048-ON, S4048-ON, S4048T-ON, S6010-ON, Z9100-ON, and S6100-ON.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the S6100-ON.
<b>9.8(2.0)</b>	Introduced on the S3100 series.
<b>9.8(1.0)</b>	Introduced on the Z9100-ON.
<b>9.8(0.0P5)</b>	Introduced on the S4048-ON.
<b>9.8(0.0P2)</b>	Introduced on the S3048-ON.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.0.2.0</b>	Introduced on the S6000.
<b>9.2(1.0)</b>	Introduced on the Z9500.
<b>9.2.(0.0)</b>	Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.
<b>9.0.0.0</b>	Introduced BFD for BGP on the Z9000.
<b>8.3.19.0</b>	Introduced on the S4820T.
<b>8.3.8.0</b>	Introduced BFD for BGP on the S4810.
<b>8.4.1.3</b>	Introduced BFD for BGP on the E-Series.
<b>8.2.1.0</b>	Introduced BFD for OSPF and ISIS on the E-Series.
<b>7.6.1.0</b>	Introduced BFD for OSPF on the C-Series.
<b>7.5.1.0</b>	Introduced BFD for ISIS on the E-Series.
<b>7.4.1.0</b>	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`).

You can enable BFD on both default and nondefault VRFs for OSPF and BGP protocols for both IPv4 and IPv6 neighbors.

 **NOTE:** The `bfd all-neighbors` command is applicable for both IPv4 and IPv6 BGP sessions.

## bfd disable

Disable BFD on an interface.

**Syntax** `bfd disable`  
Re-enable BFD using the `no bfd disable` command.

**Defaults** BFD is disabled by default.

**Command Modes** INTERFACE VRRP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## bfd enable (Configuration)

Enable BFD on all interfaces.

**Syntax** `bfd enable`  
Disable BFD using the `no bfd enable` command.

**Defaults** BFD is disabled by default.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## bfd enable (Interface)

Enable BFD on an interface.

**Syntax** `bfd enable`

**Defaults** BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## bfd interval

Specify non-default BFD session parameters beginning with the transmission interval.

**Syntax** `bfd interval interval min_rx min_rx multiplier value role {active | passive}`

Parameters		
<b>interval</b> <i>milliseconds</i>	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 <b>200</b> .	
<b>min_rx</b> <i>milliseconds</i>	Enter the keywords <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 1000. The default is <b>200</b> .	
<b>multiplier</b> <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 <b>3</b> .	
<b>role</b> [active   passive]	Enter the role that the local system assumes: <ul style="list-style-type: none"> <li>• <b>Active</b> — The active system initiates the BFD session. Both systems can be active for the same session.</li> <li>• <b>Passive</b> — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.</li> </ul> The default is <b>Active</b> .	

**Defaults** Refer to *Parameters*.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4 role
passive
Dell(conf-if-gi-0/3)#
```

## bfd protocol-liveness

Enable the BFD protocol liveness feature.

**Syntax** `bfd protocol-liveness`

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (for example, OSPF and ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.

## ip route bfd

Enable BFD for all neighbors configured through static routes.

**Syntax**

```
ip route bfd [prefix-list prefix-list-name] [interval interval min_rx min_rx multiplier value role {active | passive}]
```

To disable BFD for all neighbors configured through static routes, use the `no ip route bfd [prefix-list prefix-list-name] [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

**Parameters**

**prefix-list *prefix-list-name*** (Optional) Enter the keyword `prefix-list` followed by the name of the prefix list to enable or disable BFD on specific neighbors.

**interval *milliseconds*** (OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.

**min\_rx *milliseconds*** Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.

**multiplier *value*** Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

**role [active | passive]** Enter the role that the local system assumes:

- **Active** — 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.11(0.0)</b>	Introduced the <code>prefix-list</code> keyword.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ip ospf bfd all-neighbors

Establish BFD sessions with all OSPF neighbors on a single interface or use non-default BFD session parameters.

**Syntax** `ip ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]`

To disable all BFD sessions on an OSPF interface implicitly, use the `no ip ospf bfd all-neighbors disable` command in interface mode..

<b>Parameters</b>	<b>disable</b>	(OPTIONAL) Enter the keyword <code>disable</code> to disable BFD on this interface.
	<b>interval <i>milliseconds</i></b>	(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 <b>200</b> .
	<b>min_rx <i>milliseconds</i></b>	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 <b>200</b> .
	<b>multiplier <i>value</i></b>	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 <b>3</b> .
	<b>role [active   passive]</b>	Enter the role that the local system assumes: <ul style="list-style-type: none"><li>• <code>Active</code> — active system initiates the BFD session. Both systems can be active for the same session.</li><li>• <code>Passive</code> — passive system does not initiate a session. It only responds to a request for session initialization from the active system.</li></ul> The default is <b>Active</b> .

**Defaults** See *Parameters*.

**Command Modes** INTERFACE

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

<b>Version</b>	<b>Description</b>
<b>9.10(0.2)</b>	Introduced support for enabling BFD on non-default VRFs for OSPFv2.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.8(2.0)</b>	Introduced on the S3100 series.
<b>9.8(0.0P5)</b>	Introduced on the S4048-ON.
<b>9.8(0.0P2)</b>	Introduced on the S3048-ON.
<b>9.2.0.0</b>	Introduced on the Z9000, S4820T, and S4810.

**Usage Information** This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure `ip ospf bfd` in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword `disable`.

# ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

**Syntax** `ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]`

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]` command in interface mode..

**Parameters**

**disable** (OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.

**interval *milliseconds*** (OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.

**min\_rx *milliseconds*** Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.

**multiplier *value*** Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

**role [active | passive]** Enter the role that the local system assumes:

- **Active** — The active system initiates the BFD session. Both systems can be active for the same session.
- **Passive** — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

**Defaults** See Parameters

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# isis bfd all-neighbors

Enable BFD on all IS-IS neighbors discovered on an interface.

**Syntax** `isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]`

To remove all BFD sessions with IS-IS neighbors discovered on this interface, use the `no isis bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]` command.

**Parameters**

**disable** (OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.

**interval *milliseconds*** (OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.

**min\_rx *milliseconds*** Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is **200**.

**multiplier *value*** Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

**role [active | passive]** Enter the role that the local system assumes:

- `Active` — The active system initiates the BFD session. Both systems can be active for the same session.
- `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

**Defaults** See Parameters

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command provides the flexibility to fine-tune the timer values based on individual interface needs when ISIS BFD is configured in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if BFD is configured in CONFIGURATION mode.

To disable BFD on a specific interface while BFD is configured in CONFIGURATION mode, use the keyword `disable`.

## 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**

- ip-address*** Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
- peer-group-name*** Enter the name of the peer group that you want to explicitly enable for BFD sessions.

**Defaults** none

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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: **200** milliseconds, min\_rx: **200** 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.  
[show bfd neighbors](#) — displays the BFD neighbor information on all interfaces or a specified interface.

## neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command:

- The neighbor does not inherit the global BFD disable values configured with the `bfd all-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 all-neighbor` command: `interval`, `min_rx`, and `multiplier`.

When you remove the Disabled state of a BFD for a BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd all-neighbor` command or configured for the peer group to which the neighbor belongs.

**Related Commands**

[bfd all-neighbors](#) — enables BFD sessions with all neighbors discovered by Layer 3 protocols.  
[show bfd neighbors](#) — displays the BFD neighbor information on all interfaces or a specified interface.

## show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

**Syntax** `show bfd [vrf vrf name] neighbors [interface] [detail]`

**Parameters**

***vrf vrf name*** (Optional) Enter the keyword `vrf` and then the name of the VRF to display the BFD sessions with all neighbors within the VRF.

***interface*** (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 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 view detailed information about BFD neighbors.

**Defaults** None

- Command Modes**
- EXEC
  - EXEC Privilege

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

Version	Description
<b>9.11(2.1P1)</b>	Introduced the <code>vrf</code> keyword on all the remaining Dell EMC Networking OS platforms.
<b>9.10(0.2)</b>	Introduced the <code>vrf</code> keyword on the S3048-ON, S4048-ON, S4048T-ON, S6010-ON, Z9100-ON, and S6100-ON.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.8(2.0)</b>	Introduced on the S3100 series.
<b>9.8(0.0P5)</b>	Introduced on the S4048-ON.
<b>9.8(0.0P2)</b>	Introduced on the S3048-ON.
<b>9.2(1.0)</b>	Introduced on the Z9500.
<b>9.0.0.0</b>	Introduced on the Z9000.
<b>8.3.19.0</b>	Introduced on the S4820T.
<b>8.3.8.0</b>	Added support for BFD for BGP on the S4810.
<b>8.4.1.3</b>	Added support for BFD for BGP on the E-Series.
<b>8.2.1.0</b>	Introduced on the E-Series.
<b>7.6.1.0</b>	Introduced on the C-Series.
<b>7.5.1.0</b>	Added support for BFD for VLAN and port-channel interfaces on the E-Series.
<b>7.4.1.0</b>	Introduced BFD on physical ports on the E-Series.

**Example** The following example shows the `show bfd neighbors` command output for the default VRF.

**Example (Detail)**

- Related Commands**
- [bfd all-neighbors](#) — establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

## vrrp bfd neighbor

Establish a BFD for VRRP session with a neighbor.

**Syntax** `vrrp bfd neighbor ip-address`

**Parameters** **neighbor ip-address** Enter the IP address of the BFD neighbor.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

**Command  
History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

# Border Gateway Protocol IPv4 (BGPv4)

For detailed information about configuring 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)

BGP IPv6 Commands are listed in the following sections:

- IPv6 BGP Commands
- IPv6 MBGP Commands

## Topics:

- BGPv4 Commands
- address-family
- aggregate-address
- bgp add-path
- bgp always-compare-med
- bgp asnotation
- bgp bestpath as-path ignore
- bgp bestpath as-path multipath-relax
- bgp bestpath med confed
- bgp bestpath med missing-as-best
- bgp bestpath router-id ignore
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default local-preference
- bgp enforce-first-as
- bgp fast-external-failover
- bgp four-octet-as-support
- bgp graceful-restart
- bgp non-deterministic-med
- bgp outbound-optimization
- bgp recursive-bgp-next-hop
- bgp regex-eval-optz-disable
- bgp router-id
- bgp soft-reconfig-backup
- capture bgp-pdu neighbor
- capture bgp-pdu max-buffer-size
- clear ip bgp
- clear ip bgp dampening
- clear ip bgp flap-statistics
- clear ip bgp peer-group
- debug ip bgp
- debug ip bgp dampening
- debug ip bgp events
- debug ip bgp keepalives
- debug ip bgp notifications



- debug ip bgp soft-reconfiguration
- debug ip bgp updates
- default-metric
- description
- max-paths
- neighbor activate
- neighbor add-path
- neighbor advertisement-interval
- neighbor advertisement-start
- neighbor allowas-in
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor fall-over
- neighbor local-as
- neighbor maximum-prefix
- neighbor password
- neighbor peer-group (assigning peers)
- neighbor peer-group (creating group)
- neighbor peer-group passive
- neighbor remote-as
- neighbor remove-private-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor shutdown
- neighbor soft-reconfiguration inbound
- neighbor timers
- neighbor timers extended
- neighbor update-source
- neighbor weight
- network
- network backdoor
- redistribute
- redistribute ospf
- router bgp
- shutdown all
- shutdown address-family-ipv4–multicast
- shutdown address-family-ipv4–unicast
- shutdown address-family-ipv6–unicast
- show capture bgp-pdu neighbor
- show config
- show ip bgp
- show ip bgp cluster-list
- show ip bgp community
- show ip bgp community-list
- show ip bgp dampened-paths
- show ip bgp detail
- show ip bgp extcommunity-list
- show ip bgp filter-list
- show ip bgp flap-statistics
- show ip bgp inconsistent-as
- show ip bgp neighbors
- show ip bgp next-hop
- show ip bgp paths
- show ip bgp paths as-path

- `show ip bgp paths community`
- `show ip bgp peer-group`
- `show ip bgp regexp`
- `show ip bgp summary`
- `show running-config bgp`
- `timers bgp`
- `timers bgp extended`
- MBGP Commands
- BGP Extended Communities (RFC 4360)
- `set extcommunity rt`
- `set extcommunity soo`
- `show ip bgp paths extcommunity`
- `show ip bgp extcommunity-list`
- IPv6 BGP Commands
- `bgp soft-reconfig-backup`
- `clear ip bgp ipv6 unicast soft`
- `debug ip bgp ipv6 unicast soft-reconfiguration`
- `ipv6 prefix-list`
- `show ipv6 prefix-list`
- IPv6 MBGP Commands
- `show ipv6 mbgproutes`

## BGPv4 Commands

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 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 Version 7.7.1 supports 2-Byte (16-bit) and 4-Byte (32-bit) format for autonomous system numbers (ASNs), where the 2-Byte format is 1-65535 and the 4-Byte format is 1-4294967295.

**NOTE:** Dell Networking OS Version 8.3.1.0 supports dotted format as well as the traditional plain format for AS numbers. Display the dot format 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-Byte 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 | ipv6unicast]`

**Parameters**

- ipv4 multicast** Enter BGPv4 multicast mode.
- ipv6 unicast** Enter BGPv6 mode.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# aggregate-address

To minimize the number of entries in the routing table, summarize a range of prefixes.

<b>Syntax</b>	<code>aggregate-address ip-address mask [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]</code>	
<b>Parameters</b>	<b><i>ip-address mask</i></b>	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).
	<b><i>advertise-map map-name</i></b>	(OPTIONAL) Enter the keywords <code>advertise-map</code> then the name of a configured route map to set filters for advertising an aggregate route.
	<b><i>as-set</i></b>	(OPTIONAL) Enter the keyword <code>as-set</code> 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.
	<b><i>attribute-map map-name</i></b>	(OPTIONAL) Enter the keywords <code>attribute-map</code> then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
	<b><i>summary-only</i></b>	(OPTIONAL) Enter the keyword <code>summary-only</code> to advertise only the aggregate address. Specific routes are not advertised.
	<b><i>suppress-map map-name</i></b>	(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.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	<ul style="list-style-type: none"><li>• ROUTER BGP ADDRESS FAMILY</li><li>• ROUTER BGP ADDRESS FAMILY IPv6</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>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.</p> <p>If routes within the aggregate are constantly changing, do not add the <code>as-set</code> parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.</p> <p>In route maps used in the <code>suppress-map</code> parameter, routes meeting the <code>deny</code> clause are not suppressed; in other words, they are allowed. The opposite is also true: routes meeting the <code>permit</code> clause are suppressed.</p> <p>If the route is injected via the <code>network</code> command, that route still appears in the routing table if the <code>summary-only</code> parameter is configured in the <code>aggregate-address</code> command.</p> <p>The <code>summary-only</code> parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the <code>neighbor distribute-list</code> command.</p> <p>In the <code>show ip bgp</code> command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.</p>	

# 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] path-count`

<b>Parameters</b>	<b>send</b>	Enter the keyword <code>send</code> to indicate that the system sends multiple paths to peers.
	<b>receive</b>	Enter the keyword <code>receive</code> to indicate that the system accepts multiple paths from peers.
	<b>both</b>	Enter the keyword <code>both</code> to indicate that the system sends and accepts multiple paths from peers.
	<b><i>path-count</i></b>	Enter the number paths supported. The range is from 2 to 64.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>ROUTER BGP</li> <li>ROUTER BGP-address-family</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<code>neighbor add-path</code> — 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.

<b>Syntax</b>	<code>bgp always-compare-med</code>	
	To disable comparison of MED, enter <code>no bgp always-compare-med</code> .	
<b>Defaults</b>	Disabled (that is, the software only compares MEDs from neighbors within the same AS).	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Any update without a MED attribute is the least preferred route.	
	If you enable this command, use the <code>clear ip bgp *</code> command to recompute the best path.	

## bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

<b>Syntax</b>	<code>bgp asnotation [asplain   asdot+   asdot]</code>	
	To disable a dot or dot+ representation and return to ASPLAIN, enter the <code>no bgp asnotation</code> command.	
<b>Defaults</b>	<b>asplain</b>	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>Before enabling this feature, enable the <code>enable bgp four-octet-as-support</code> command. If you disable the <code>four-octet-support</code> command after using <code>dot</code> or <code>dot+</code> format, the AS numbers revert to asplain text.</p> <p>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.</p>						

**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.

<b>Syntax</b>	<pre>bgp bestpath as-path ignore</pre> <p>To return to the default, enter the <code>no bgp bestpath as-path ignore</code> command.</p>
<b>Defaults</b>	Disabled (that is, the software considers the AS_PATH when choosing a route as best).
<b>Command Modes</b>	ROUTER BGP
<b>Supported Modes</b>	Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**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** `bgp bestpath as-path multipath-relax`  
To return to the default BGP routing process, use the `no bgp bestpath as-path multipath-relax` command.

**Defaults** Disabled

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `bgp bestpath med confed`  
To disable MED comparison on BGP confederation paths, enter the `no bgp bestpath med confed` command.

**Defaults** Disabled

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

<b><i>ip-address</i></b>	Enter an IP address as the route reflector cluster ID.
<b><i>number</i></b>	Enter a route reflector cluster ID as a number from 1 to 4294967295.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

**Related Commands**

- [bgp client-to-client reflection](#) — enables route reflection between the route reflector and clients.
- [neighbor route-reflector-client](#) — configures a route reflector and clients.
- [show ip bgp cluster-list](#) — views paths with a cluster ID.

## bgp confederation identifier

Configure an identifier for a BGP confederation.

**Syntax** `bgp confederation identifier as-number`  
To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

**Parameters**

<b><i>as-number</i></b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.



The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGP peers without a LOCAL\_PREF attribute. The software sends AS\_CONFED\_SET and accepts AS\_CONFED\_SET and AS\_CONF\_SEQ.

**Related Commands** [bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

## bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

**Syntax** `bgp confederation peers as-number [...as-number]`

To return to the default, use the `no bgp confederation peers` command.

**Parameters**

<b><i>as-number</i></b>	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).
<b><i>...as-number</i></b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]`

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

**Parameters**

<b><i>half-life</i></b>	(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 <b>15 minutes</b> .
-------------------------	--

<b>reuse</b>	(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 <b>750</b> .
<b>suppress</b>	(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 <b>2000</b> .
<b>max-suppress-time</b>	(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 <b>60 minutes</b> .
<b>route-map map-name</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you enter the `bgp dampening` command, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent; therefore, if you configure one parameter, configure the parameters in the order they appear in the CLI.

**Related Commands** [show ip bgp dampened-paths](#) — views the BGP paths.

## bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	All routers apply the <code>bgp default local-preference</code> command setting within the AS. To set the local preference for a specific route, use the <code>set local-preference</code> command in ROUTE-MAP mode.
<b>Related Commands</b>	<a href="#">set metric</a> — assigns a local preference value for a specific route.

## bgp enforce-first-as

Disable (or enable) `enforce-first-as` check for updates received from EBGp peers.

<b>Syntax</b>	<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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	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. To view the “failed enforce-first-as check” counter, use the <code>show ip bgp neighbors</code> command.  If you disable the <code>enforce-first-as</code> command, it can be viewed using the <code>show ip protocols</code> command.
--------------------------	---

<b>Related Commands</b>	<a href="#">show ip bgp neighbors</a> — views the information the BGP neighbors exchange. <a href="#">show ip protocols</a> — views information on routing protocols.
-------------------------	--

## bgp fast-external-failover

Enable the fast external failover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

<b>Syntax</b>	<code>bgp fast-external-failover</code> To disable fast external failover, use the <code>no bgp fast-external-failover</code> command.
---------------	---

**Defaults** Enabled

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	The <code>bgp fast-external-failover</code> command appears in the <code>show config</code> command output.
--------------------------	---

## bgp four-octet-as-support

Enable 4-byte support for the BGP process.

**Syntax** `bgp four-octet-as-support`  
To disable fast external failover, use the `no bgp four-octet-as-support` command.

**Defaults** Disabled (supports 2-byte format)

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router.

When creating Confederations, all the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

Where the 2-byte format is from 1 to 65535, the 4-byte format is from 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format.

For more information about using the 2 byte or 4-byte format, refer to the *Dell Networking OS Configuration Guide*.

## bgp graceful-restart

To support graceful restart as a receiver only, enable graceful restart on a BGP neighbor, a BGP node, or designate a local router.

**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	Parameter	Description
	<b>restart-time seconds</b>	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 <b>120 seconds</b> .
	<b>stale-path-time seconds</b>	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 <b>360 seconds</b> .
	<b>role receiver-only</b>	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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

## bgp 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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

## bgp outbound-optimization

Enables outbound optimization for IBGP peer-group members.

**Syntax** `bgp outbound-optimization`

To disable outbound optimization, enter the `no bgp outbound-optimization` command.

**Defaults** Enabled.

**Command Modes** ROUTER BGP

**Command History**

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

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

**Version**

**Description**

**9.4.(0.0)**

Introduced on the S4810.

**9.2(1.0)**

Introduced on the Z9500.

**Usage Information**

The updates are sent to all the neighbors in the peer-group and all the neighbors have the same attributes including next-hop.

Enabling or disabling outbound optimization dynamically resets all neighbor sessions.

When you enable outbound optimization, all peers receive the same update packets. Also, the next-hop address, which is chosen as one of the addresses of the neighbor's reachable interface, is the same for all peers.

# bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

**Syntax** `bgp recursive-bgp-next-hop`  
To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults** Enabled

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is a *knob* to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

**Related Commands** `clear ip bgp` — clears the ip bgp.

# bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

**Syntax** `bgp regex-eval-optz-disable`  
To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

**Defaults** Enabled

**Command Modes** ROUTER BGP (conf-router\_bgp)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## bgp router-id

Assign a user-given ID to a BGP router.

**Syntax** `bgp router-id ip-address`  
 To delete a user-assigned IP address, use the `no bgp router-id` command.

**Parameters** *ip-address* Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults** The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Peering sessions are reset when you change the router ID of a BGP router.

## bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

**Syntax** `bgp soft-reconfig-backup`  
 To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults** **Off**

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

### Related Commands

[clear ip bgp](#) — activates inbound policies without resetting the BGP TCP session.

## capture bgp-pdu neighbor

Enable capture of an IPv4 BGP neighbor packet.

### Syntax

```
capture bgp-pdu neighbor ipv4-address direction {both | rx | tx}
```

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

### Parameters

***ipv4-address*** Enter the IPv4 address of the target BGP neighbor.

***direction {both | rx | tx}*** Enter the keyword `direction` and a direction — either `rx` for inbound, `tx` for outbound, or `both`.

### Defaults

Not configured.

### Command Modes

EXEC Privilege

### Supported Modes

Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Related Commands

[capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

[show capture bgp-pdu neighbor](#) — displays BGP packet capture information.

## capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

### Syntax

```
capture bgp-pdu max-buffer-size 100-102400000
```

### Parameters

***100-102400000*** Enter a size for the capture buffer.

### Defaults

40960000 bytes.

### Command Modes

EXEC Privilege

### Supported Modes

Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Related Commands

[capture bgp-pdu neighbor](#) — enables capture of an IPv4 BGP neighbor packet.


[show capture bgp-pdu neighbor](#) — displays BGP packet capture information for an IPv6 address.



# clear ip bgp

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax** `clear ip bgp * | as-number | ip-address [flap-statistics | soft [in | out]]`

<b>Parameters</b>	<b>*</b>	Enter an asterisk ( * ) to reset all BGP sessions.
	<b>as-number</b>	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).
	<b>ip-address</b>	Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
	<b>flap-statistics</b>	(OPTIONAL) Enter the keyword <code>flap-statistics</code> to reset the flap statistics on all prefixes from that neighbor.
	<b>soft</b>	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.  <b>NOTE:</b> If you enter the <code>clear ip bgp ip-address soft</code> command, both inbound and outbound policies are reset.
	<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
	<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [bgp recursive-bgp-next-hop](#) — disables next-hop resolution through other routes learned by the BGP.  
[bgp soft-reconfig-backup](#) — turns on BGP Soft Reconfiguration.

# clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

**Syntax** `clear ip bgp dampening [ip-address mask]`

<b>Parameters</b>	<b>ip-address mask</b>	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.
-------------------	------------------------	---

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.

# 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 flap-statistics [ip-address mask | filter-list as-path-name | regex regular-expression]`

**Parameters**

- ip-address mask*** (OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) 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.
- regex regular-expression*** (OPTIONAL) Enter the keyword `regex` 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 peer-group peer-group-name`

**Parameters** ***peer-group-name*** Enter the peer group name to reset the BGP sessions within that peer group.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

**Syntax** `debug ip bgp [ip-address | peer-group peer-group-name] [in | out]`  
 To disable all BGP debugging, use the `no debug ip bgp` command.

**Parameters**

- ip-address*** Enter the IP address of the neighbor in dotted decimal format.
- peer-group peer-group-name*** Enter the keywords `peer-group` then the name of the peer group to debug.
- in*** (OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
- out*** (OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 dampening [in | out]`  
 To disable debugging, use the `no debug ip bgp dampening` command.

**Parameters**

- in*** (OPTIONAL) Enter the keyword `in` to view only inbound dampened routes.
- out*** (OPTIONAL) Enter the keyword `out` to view only outbound dampened routes.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [show debugging](#) — view enabled debugging operations.  
[show ip bgp dampened-paths](#) — view BGP dampened routes.

## debug ip bgp events

Display information on local BGP state changes and other BGP events.

**Syntax** `debug ip bgp [ip-address | peer-group peer-group-name] events [in | out]`  
To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] events` command.

**Parameters**

- ip-address*** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group *peer-group-name*** (OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
- in** (OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
- out** (OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [ip-address | peer-group peer-group-name] keepalives [in | out]`  
To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

**Parameters**

- ip-address*** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group *peer-group-name*** (OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
- in** (OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
- out** (OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [ip-address | peer-group peer-group-name] notifications [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

<b>Parameters</b>		
<b><i>ip-address</i></b>	(OPTIONAL)	Enter the IP address of the neighbor in dotted decimal format.
<b><i>peer-group peer-group-name</i></b>	(OPTIONAL)	Enter the keyword <code>peer-group</code> then the name of the peer group.
<b>in</b>	(OPTIONAL)	Enter the keyword <code>in</code> to view BGP notifications received from neighbors.
<b>out</b>	(OPTIONAL)	Enter the keyword <code>out</code> to view BGP notifications sent to neighbors

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 {ip-address | peer-group-name} soft-reconfiguration`

To disable, use the `no debug ip bgp {ip-address | peer-group-name} soft-reconfiguration` command.

<b>Parameters</b>		
<b><i>ip-address</i></b>	(OPTIONAL)	Enter the IP address of the neighbor in dotted decimal format.
<b><i>peer-group-name</i></b>	(OPTIONAL)	Enter the name of the peer group to disable or enable all routers within the peer group..

**Defaults** Disabled

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] updates [in | out]` command.

Parameters		
	<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.
	<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.
	<b>prefix-list prefix-list-name</b>	(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 <b>permit</b> (to allow all routes).
	<b>ip-address</b>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<b>peer-group-name</b>	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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		
	<b>number</b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	The <code>default-metric</code> command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.	
<b>Related Commands</b>	<a href="#">bgp always-compare-med</a> — enables comparison of all BGP MED attributes. <a href="#">redistribute</a> — redistributes routes from other routing protocols into BGP.	

## description

Enter a description of the BGP routing protocol

<b>Syntax</b>	<code>description {description}</code>	
	To remove the description, use the <code>no description {description}</code> command.	
<b>Parameters</b>	<b><i>description</i></b>	Enter a description to identify the BGP protocol (80 characters maximum).
<b>Defaults</b>	none	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**     [router bgp](#) — enters ROUTER mode on the switch.

## max-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

<b>Syntax</b>	<code>max-paths {ebgp   ibgp} number</code>	
	To return to the default values, enter the <code>no maximum-paths</code> command.	
<b>Parameters</b>	<b><i>ebgp</i></b>	Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.
	<b><i>ibgp</i></b>	Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes.
	<b><i>number</i></b>	Enter a number as the maximum number of parallel paths. The range is from 2 to 64.
<b>Defaults</b>	none	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** (OPTIONAL) Enter the name of the peer group.
- activate** Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

**Defaults** Disabled

**Command Modes** CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. When you use `activate` in the new context, the neighbor/peer group enables for AFI/SAFI.

# neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

**Syntax** `neighbor [ip-address | peer-group-name] add-path [send | receive | both] count`

**Parameters**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** (OPTIONAL) Enter the name of the peer group.
- send** Enter the keyword `send` to indicate that the system sends multiple paths to peers.
- receive** Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
- both** Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
- count** Enter the number paths supported. The range is from 2 to 64.

**Defaults** none

**Command Modes** CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- seconds** Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

**Defaults**

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- seconds** Enter a number as the time interval, in seconds, before BGP route updates are sent. The range is from 0 to 3600 seconds.

**Defaults** none

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

# neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

**Syntax** `neighbor {ip-address | peer-group-name} allowas-in number`  
To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

**Parameters**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- number** Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `neighbor {ip-address | peer-group-name} default-originate [route-map map-name]`  
To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

**Parameters**

- ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** Enter the name of the peer group to set the default route of all routers in that peer group.
- route-map map-name** (OPTIONAL) Enter the keyword `route-map` then the name of a configured route map.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

# neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

**Syntax** `neighbor {ip-address | peer-group-name} description text`  
To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

**Parameters**

- ip-address** Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** Enter the name of the peer group.
- text** Enter a continuous text string up to 80 characters.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# 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**

- ip-address** Enter the IP address of the neighbor in dotted decimal format.
- peer-group-name** Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
- prefix-list-name** Enter the name of an established prefix list.  
If the prefix list is not configured, the default is **permit** (to allow all routes).
- in** Enter the keyword `in` to distribute only inbound traffic.
- out** Enter the keyword `out` to distribute only outbound traffic.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>neighbor {ip-address   peer-group-name} ebgp-multihop [ttl]</code> To disallow and disconnect connections, use the <code>no neighbor {ip-address   peer-group-name} ebgp-multihop</code> command.						
<b>Parameters</b>	<p><b>ip-address</b> Enter the IP address of the neighbor in dotted decimal format.</p> <p><b>peer-group-name</b> Enter the name of the peer group.</p> <p><b>ttl</b> (OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is from 1 to 255. The default is <b>255</b>.</p>						
<b>Defaults</b>	Disabled.						
<b>Command Modes</b>	ROUTER BGP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	To prevent loops, the <code>neighbor ebgp-multihop</code> 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.

<b>Syntax</b>	<code>neighbor {ipv4-address   peer-group-name} fall-over</code> To disable, use the <code>no neighbor {ipv4-address   peer-group-name} fall-over</code> command.						
<b>Parameters</b>	<p><b>ipv4-address</b> Enter the IP address of the neighbor in dotted decimal format.</p> <p><b>peer-group-name</b> Enter the name of the peer group.</p>						
<b>Defaults</b>	Disabled.						
<b>Command Modes</b>	ROUTER BGP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.						
<b>Related Commands</b>	<a href="#">show ip bgp neighbors</a> — 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.

<b>Syntax</b>	<code>neighbor {ip-address   peer-group-name} local-as as-number [no-prepend]</code> To return to the default value, use the <code>no neighbor {ip-address   peer-group-name} local-as</code> command.						
<b>Parameters</b>	<p><b>ip-address</b> Enter the IP address of the neighbor in dotted decimal format.</p> <p><b>peer-group-name</b> Enter the name of the peer group to set the advertisement interval for all routers in the peer group.</p> <p><b>as-number</b> 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).</p> <p><b>no prepend</b> Specifies that local AS values do not prepend to announcements from the neighbor.</p>						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	ROUTER BGP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<a href="#">bgp four-octet-as-support</a> — enables 4-byte support for the BGP process.						

# neighbor maximum-prefix

Control the number of network prefixes received.

<b>Syntax</b>	<code>neighbor {ip-address   peer-group-name} maximum-prefix maximum [threshold] [warning-only]</code> To return to the default values, use the <code>no neighbor {ip-address   peer-group-name} maximum-prefix maximum</code> command.
<b>Parameters</b>	<p><b>ip-address</b> Enter the IP address of the neighbor in dotted decimal format.</p> <p><b>peer-group-name</b> Enter the name of the peer group.</p> <p><b>maximum</b> Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.</p> <p><b>threshold</b> (OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is <b>75</b>.</p> <p><b>warning-only</b> (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.</p>
<b>Defaults</b>	threshold = <b>75</b>
<b>Command Modes</b>	ROUTER BGP
<b>Supported Modes</b>	Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	If you configure the <code>neighbor maximum-prefix</code> command and the neighbor receives more prefixes than the <code>neighbor maximum-prefix</code> command configuration allows, the neighbor goes down and the <code>show ip bgp summary</code> command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the <code>clear ip bgp</code> command for the neighbor or the peer group to which the neighbor belongs or you enter the <code>neighbor shutdown</code> and <code>neighbor no shutdown</code> commands.						
<b>Related Commands</b>	<a href="#">show ip bgp summary</a> — 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**

- ip-address*** Enter the IP address of the router to be included in the peer group.
- peer-group-name*** Enter the name of a configured peer group.
- encryption-type*** (OPTIONAL) Enter 7 as the encryption type for the password entered. 7 means that the password is encrypted and hidden.
- password*** Enter a text string up to 80 characters long. The first character of the password must be a letter.  
You cannot use spaces in the password.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**Usage Information**

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from  
[peer's IP address] : 11502 to [local router's IP address] :179
```

## neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

**Syntax** `neighbor ip-address peer-group peer-group-name`  
To delete a peer from a peer group, use the `no neighbor ip-address peer-group peer-group-name` command.

**Parameters**  
***ip-address*** Enter the IP address of the router to be included in the peer group.  
***peer-group-name*** Enter the name of a configured peer group.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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](#)
- [neighbor shutdown](#)

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

**Related Commands**  
[clear ip bgp](#) — resets BGP sessions.  
[neighbor peer-group \(creating group\)](#) — creates a peer group.  
[show ip bgp peer-group](#) — views BGP peers.  
[show ip bgp neighbors](#) — views BGP neighbors configurations.

## neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

**Syntax** `neighbor peer-group-name peer-group`  
To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

<b>Parameters</b>	<b><i>peer-group-name</i></b>	Enter a text string up to 16 characters long as the name of the peer group.
<b>Defaults</b>		Not configured.
<b>Command Modes</b>		ROUTER BGP
<b>Supported Modes</b>		Full-Switch
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>		When you create a peer group, it is disabled (Shut mode).
<b>Related Commands</b>		<a href="#">neighbor peer-group (assigning peers)</a> — assigns routers to a peer group. <a href="#">neighbor remote-as</a> — assigns an indirectly connected AS to a neighbor or peer group. <a href="#">neighbor shutdown</a> — 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.

<b>Syntax</b>	<code>neighbor <i>peer-group-name</i> peer-group passive [<i>limit sessions</i>]</code>
	To delete a passive peer-group, use the <code>no neighbor <i>peer-group-name</i> peer-group passive</code> command.
<b>Parameters</b>	<p><b><i>peer-group-name</i></b> Enter a text string up to 16 characters long as the name of the peer group.</p> <p><b><i>limit</i></b> (Optional) Enter the keyword <code>limit</code> to constrain the numbers of sessions for this peer-group. The range is from 2 to 256. The default is <b>256</b>.</p>
<b>Defaults</b>	Not configured.
<b>Command Modes</b>	ROUTER BGP
<b>Supported Modes</b>	Full-Switch
<b>Command History</b>	<b>Version</b>
	<b>9.9(0.0)</b>
	<b>9.2(0.0)</b>
<b>Usage Information</b>	<p>After you configure a peer group as passive, assign it a subnet using the <code>neighbor soft-reconfiguration inbound</code> command.</p> <p>For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.</p>
<b>Related Commands</b>	<p><a href="#">neighbor soft-reconfiguration inbound</a> — assigns a subnet to a dynamically configured BGP neighbor.</p> <p><a href="#">neighbor remote-as</a> — assigns an indirectly connected AS to a neighbor or peer group.</p>

## neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

<b>Syntax</b>	<code>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} remote-as <i>number</i></code>
---------------	--



To delete a remote AS entry, use the `no neighbor {ip-address | peer-group-name} remote-as number` command.

<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the IP address of the neighbor to enter the remote AS in its routing table.
	<b><i>peer-group-name</i></b>	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
	<b><i>number</i></b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To accept 4-byte formats before entering a 4 byte AS Number, configure your system. If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (Shutdown).

**Related Commands** [router bgp](#) — enters ROUTER BGP mode and configures routes in an AS.  
[bgp four-octet-as-support](#) — enables 4-byte support for the BGP process.

## neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

**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.

<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the IP address of the neighbor to remove the private AS numbers.
	<b><i>peer-group-name</i></b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

<b><i>ip-address</i></b>	Enter the IP address of the neighbor in dotted decimal format.
<b><i>peer-group-name</i></b>	Enter the name of the peer group.
<b><i>map-name</i></b>	Enter the name of an established route map. If the Route map is not configured, the default is <b>deny</b> (to drop all routes).
<b>in</b>	Enter the keyword <code>in</code> to filter inbound routes.
<b>out</b>	Enter the keyword <code>out</code> to filter outbound routes.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

<b><i>ip-address</i></b>	Enter the IP address of the neighbor in dotted decimal format.
<b><i>peer-group-name</i></b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not to be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

**Related Commands**

[bgp client-to-client reflection](#) — enables route reflection between the route reflector and the clients.

## neighbor shutdown

Disable a BGP neighbor or peer group.

<b>Syntax</b>	<code>neighbor {ip-address   peer-group-name} shutdown</code>	
	To enable a disabled neighbor or peer group, use the <code>neighbor {ip-address   peer-group-name} no shutdown</code> command.	
<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the IP address of the neighbor in dotted decimal format.
	<b><i>peer-group-name</i></b>	Enter the name of the peer group to disable or enable all routers within the peer group.
<b>Defaults</b>	Enabled (that is, BGP neighbors and peer groups are disabled.)	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Peers that are enabled within a peer group are disabled when their peer group is disabled.	
	The <code>neighbor shutdown</code> 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 <code>show ip bgp summary</code> command to confirm its status.	
<b>Related Commands</b>	<a href="#">show ip bgp summary</a> — displays the current BGP configuration.	
	<a href="#">show ip bgp neighbors</a> — displays the current BGP neighbors.	

## neighbor soft-reconfiguration inbound

Enable soft-reconfiguration for BGP.

<b>Syntax</b>	<code>neighbor {ip-address   peer-group-name} soft-reconfiguration inbound</code>
---------------	---

To disable, use the `no neighbor {ip-address | peer-group-name} soft-reconfiguration inbound` command.

<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the IP address of the neighbor in dotted decimal format.
	<b><i>peer-group-name</i></b>	Enter the name of the peer group to disable or enable all routers within the peer group.


**Defaults** Disabled


**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates the neighbor receives but does not reset the peer-session.

 **CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.**

 **NOTE:** This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

**Related Commands** [show ip bgp neighbors](#) — displays routes received by a neighbor.

## neighbor 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.

<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the IP address of the peer router in dotted decimal format.
	<b><i>peer-group-name</i></b>	Enter the name of the peer group to set the timers for all routers within the peer group.
	<b><i>keepalive</i></b>	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 <b>60 seconds</b> .
	<b><i>holdtime</i></b>	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 <b>180 seconds</b> .

**Defaults**

- keepalive = **60 seconds**
- holdtime = **180 seconds**

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with any other command.

When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values are as follows:

- the lower of the `holdtime` value is the new `holdtime` value, and
- whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value, is the new `keepalive` value.

# neighbor timers extended

Set idle hold time for a BGP neighbor or a peer group.

## Syntax

```
neighbor {ip-address | ipv6-address | peer-group-name} timers extended idle holdtime
```

To return to the default values, use the `no neighbor {ip-address | ipv6-address | peer-group-name} timers extended idle holdtime` command.

## Parameters

- |   |   |
|---|---|
| <b><i>ip-address</i></b>                    | Enter the IP address of the peer router in dotted decimal format.   |
| <b><i>ipv6-address</i></b>                  | Enter the IPv6 address of the peer router in X:X:X::X format.   |
| <b><i>peer-group-name</i></b>               | Enter the name of the peer group to set the timers for all routers within the peer group.   |
| <b><i>timers extended idle holdtime</i></b> | Enter a number for the time interval, in seconds, for the peer to be idle state. The range is from 1 to 32767. The default is <b>15 seconds</b> . |

## Defaults

The default idle holdtime is **15 seconds**.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

## Command History

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

Version	Description
9.14(0.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, and S6000-ON.

## Usage Information

The peer remains in idle state based on the configured `idle holdtime`. The less the `idle holdtime`, less the peer in idle state.

For the new `idle holdtime` to take effect, you need to shutdown the respective peer manually using `neighbor shutdown` command and enable the peer again.

# neighbor update-source

Enable the 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

- |                               |  |
|-------------------------------|--|
| <b><i>ip-address</i></b>      | Enter the IP address of the peer router in dotted decimal format.              |
| <b><i>peer-group-name</i></b> | Enter the name of the peer group to disable all routers within the peer group. |

**interface** Enter the keyword `loopback` then a number of the Loopback interface. The range is from 0 to 16383.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

## neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

**Syntax** `neighbor {ip-address | peer-group-name} weight weight`  
To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

**Parameters**

- ip-address** Enter the IP address of the peer router in dotted decimal format.
- peer-group-name** Enter the name of the peer group to disable all routers within the peer group.
- weight** Enter a number as the weight. The range is from 0 to 65535. The default is **0**.


**Defaults** **0**

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** In the system best path selection process, the path with the highest weight value is preferred.

 **NOTE:** In the system 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.

## 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**

- ip-address** Enter an IP address in dotted decimal format of the network.

**mask** Enter the mask of the IP address in the slash prefix length format (for example, /24).  
The mask appears in command outputs in dotted decimal format (A.B.C.D).

**route-map map-name** (OPTIONAL) Enter the keyword `route-map` then the name of an established route map.

Only the following ROUTE-MAP mode commands are supported:

- [match ip address](#)
- [set metric](#)
- [set tag](#)

If the route map is not configured, the default is **deny** (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system 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.

**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**

**ip-address** Enter an IP address in dotted decimal format of the network.

**mask** Enter the mask of the IP address in the slash prefix length format (for example, /24).  
The mask appears in command outputs in dotted decimal format (A.B.C.D).

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Although the system does not generate a route due to the backdoor config, there is an option for injecting/sourcing a local route in the presence of network backdoor config on a learned route.

# redistribute

Redistribute routes into BGP.

<b>Syntax</b>	<code>redistribute {connected   static} [route-map <i>map-name</i>]</code> To disable redistribution, use the <code>no redistribute {connected   static}</code> command.						
<b>Parameters</b>	<table><tr><td><b>connected</b></td><td>Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.</td></tr><tr><td><b>static</b></td><td>Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.</td></tr><tr><td><b>route-map <i>map-name</i></b></td><td>(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:<ul style="list-style-type: none"><li>• <a href="#">match ip address</a></li><li>• <a href="#">set metric</a></li><li>• <a href="#">set tag</a></li></ul>If the route map is not configured, the default is <b>deny</b> (to drop all routes).</td></tr></table>	<b>connected</b>	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.	<b>static</b>	Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.	<b>route-map <i>map-name</i></b>	(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: <ul style="list-style-type: none"><li>• <a href="#">match ip address</a></li><li>• <a href="#">set metric</a></li><li>• <a href="#">set tag</a></li></ul> If the route map is not configured, the default is <b>deny</b> (to drop all routes).
<b>connected</b>	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.						
<b>static</b>	Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.						
<b>route-map <i>map-name</i></b>	(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: <ul style="list-style-type: none"><li>• <a href="#">match ip address</a></li><li>• <a href="#">set metric</a></li><li>• <a href="#">set tag</a></li></ul> If the route map is not configured, the default is <b>deny</b> (to drop all routes).						

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

With the Dell Networking OS version 8.3.1.0 and later, 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.

**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**

<b><i>process-id</i></b>	Enter the number of the OSPF process. The range is from 1 to 65535.
<b>match external {1   2}</b>	(OPTIONAL) Enter the keywords <code>match external</code> to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.



**match internal** (OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.

**route-map *map-name*** (OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** With the Dell Networking OS version 8.3.1.0 and later, you can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and apply outbound to an EBGp peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

When you enter the `redistribute isis process-id` command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. RFC does not support this feature.

## router bgp

To configure and enable BGP, enter ROUTER BGP mode.

**Syntax** `router bgp as-number`  
 To disable BGP, use the `no router bgp as-number` command.

**Parameters** ***as-number*** Enter the AS number. The range is from 1 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

**Defaults** Not enabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** At least one interface must be in Layer 3 mode for the `router bgp` command to be accepted. If no interfaces are enabled for Layer 3, an error message appears:

```
% Error: No router id
configured
```

**Example**

```
Dell(conf)#router bgp 3
Dell(conf-router_bgp)#
```

# shutdown all

Disables all the BGP neighbors.

**Syntax**                    `shutdown all`  
Use the `no shutdown all` command to enable all the configured BGP neighbors.

**Command Modes**    ROUTER BGP

<b>Command History</b>	<b>Version</b>	Description
	<b>9.11.0.0</b>	Introduced on the S-Series, Z-Series, MXL, and IOM.

**Usage Information**        You can use this command to disable all the configured BGP neighbors.  
This command is global for all VRFs.

# shutdown address-family-ipv4-multicast

Disables all the BGP neighbors corresponding to the multicast IPv4 address families.

**Syntax**                    `shutdown address-family-ipv4-multicast`  
Use the `no shutdown address-family-ipv4-multicast` command to enable all the configured BGP neighbors corresponding to the multicast IPv4 address families.

**Command Modes**    ROUTER BGP  
CONFIGURATION

<b>Command History</b>	<b>Version</b>	Description
	<b>9.11.0.0</b>	Introduced on the S-Series, Z-Series, MXL, and IOM.

**Usage Information**        You can use this command to disable all the configured BGP neighbors corresponding to the multicast IPv4 address families.  
This command is global for all VRFs.

# shutdown address-family-ipv4-unicast

Disables all the BGP neighbors corresponding to the unicast IPv4 address families.

**Syntax**                    `shutdown address-family-ipv4-unicast`  
Use the `no shutdown address-family-ipv4-unicast` command to enable all the configured BGP neighbors corresponding to the unicast IPv4 address families.

**Command Modes**    ROUTER BGP  
CONFIGURATION

<b>Command History</b>	<b>Version</b>	Description
	<b>9.11.0.0</b>	Introduced on the S-Series, Z-Series, MXL, and IOM.

**Usage Information**        You can use this command to disable all the configured BGP neighbors corresponding to the unicast IPv4 address families.  
This command is global for all VRFs.

# shutdown address-family-ipv6-unicast

Disables all the BGP neighbors corresponding to the unicast IPv6 address families.

<b>Syntax</b>	<code>shutdown address-family-ipv6-unicast</code>	
	Use the <code>no shutdown address-family-ipv6-unicast</code> command to enable all the configured BGP neighbors corresponding to the unicast IPv6 address families.	
<b>Command Modes</b>	ROUTER BGP CONFIGURATION	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.11.0.0</b>	Introduced on the S-Series, Z-Series, MXL, and IOM.
<b>Usage Information</b>	You can use this command to disable all the configured BGP neighbors corresponding to the unicast IPv6 address families.  This command is global for all VRFs.	

# show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

<b>Syntax</b>	<code>show capture bgp-pdu neighbor ipv4-address</code>	
<b>Parameters</b>	<b>ipv4-address</b>	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using 680 bytes
PDU[1] : len 101, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00650100 00000013 00000000
00000000 419ef06c 00000000
  00000000 00000000 00000000 00000000 0181a1e4 0181a25c 41af92c0
00000000 00000000 00000000
  00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
PDU[2] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
PDU[3] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
[. . .]

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using 562 bytes
PDU[1] : len 41, captured 00:34:52 ago
  ffffffff ffffffff ffffffff ffffffff 00290104 000100b4 14141401
0c020a01 04000100 01020080
  00000000
PDU[2] : len 19, captured 00:34:51 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
```

```
PDU[3] : len 19, captured 00:34:50 ago
  ffffffff ffffffff ffffffff ffffffff 00130400
[. . .]
Dell#
```

**Related Commands**

[capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

## show config

View the current ROUTER BGP configuration.

**Syntax** show config

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-router_bgp)#show config
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
Dell(conf-router_bgp)#
```

**Related Commands**

[capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

## show ip bgp

View the current BGP IPv4 routing table for the system.

**Syntax** show ip bgp [ipv4 {unicast | multicast} | ipv6 {unicast}] [network [network-mask] [longer-prefixes]] [cluster-list cluster-id] [community community-number] [community-list community-list-name] [dampened-paths] [extcommunity-list list name] [filter-list as-path-name] [flap-statistics [ip-address [mask]]] [neighbors [all {received-routes}]] [next-hop] [paths] [peer-group peer-group-name] [regex regular-expression] [summary]

**Parameters**

<b>ipv4 unicast</b>	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
<b>ipv4 multicast</b>	(OPTIONAL) Enter the keywords <code>ipv4 multicast</code> to view information only related to ipv4 multicast routes.
<b>ipv6 unicast</b>	(OPTIONAL) Enter the keywords <code>ipv6 unicast</code> to view information only related to ipv6 unicast routes.
<b>network</b>	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.

<b><i>network-mask</i></b>	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
<b>longer-prefixes</b>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
<b>cluster-list <i>cluster-id</i></b>	(OPTIONAL) Enter the keyword <code>cluster-list</code> then the cluster-ID to display the routes matching the cluster.
<b>community <i>community-number</i></b>	(OPTIONAL) Enter the keyword <code>community</code> then the <code>community-number</code> to display the routes matching the communities.
<b>community-list <i>community-list-name</i></b>	(OPTIONAL) Enter the keyword <code>community-list</code> then the <code>community-list-name</code> to display the routes matching the <code>community-list</code> .
<b>dampened-paths</b>	(OPTIONAL) Enter the keyword <code>dampened-paths</code> to display the paths suppressed due to dampening.
<b>extcommunity-list <i>list name</i></b>	(OPTIONAL) Enter the keyword <code>extcommunity-list</code> then the list name to display the routes matching the extended community-list.
<b>filter-list <i>as-path-name</i></b>	(OPTIONAL) Enter the keyword <code>filter-list</code> then the <code>as-path-name</code> to display the routes conforming to the filter-list.
<b>flap-statistics</b>	(OPTIONAL) Enter the keyword <code>flap-statistics</code> to display flap statistics of the routes.
<b>neighbors</b>	(OPTIONAL) Enter the keyword <code>neighbors</code> to display the detailed information on TCP and BGP neighbor connections.
<b>neighbors [all {received-routes}]</b>	(OPTIONAL) Enter the keyword <code>neighbors [all {received-routes}]</code> to display all the received routes both accepted and rejected from all the IPv4 or IPv6 neighbors.
<b>next-hop</b>	(OPTIONAL) Enter the keyword <code>next-hop</code> to view all the next-hop information on the learnt routes.
<b>paths</b>	(OPTIONAL) Enter the keyword <code>paths</code> to view the BGP path attributes in the BGP database.
<b>peer-group <i>peer-group-name</i></b>	(OPTIONAL) Enter the keyword <code>peer-group</code> then the <code>peer-group-name</code> to view the information on the BGP peers in a peer group.
<b>regex <i>regular-expression</i></b>	(OPTIONAL) Enter the keyword <code>regex</code> then the regular expressions to display BGP information based on a regular expression.
<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to display the summary of BGP neighbor status.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.14(0.0)</b>	Introduced the <code>[all {received-routes}]</code> option for IPv4 and IPv6 neighbors.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

The following describes the `show ip bgp` command shown in the following example.

Field	Description
<b>Network</b>	Displays the destination network prefix of each BGP route.
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	Lists all the ASs the route passed through to reach the destination network.

### Example

```
Dell EMC> show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf Weight Path
*>  0.0.0.0/0        63.114.8.33          0 18508 i
*   3.0.0.0/8        63.114.8.33          0 18508 209 701 80 i
*>  3.3.0.0/16       63.114.8.33          0 18508 701 80 i
*>  3.3.0.0/16       0.0.0.0            22      32768 ?
   63.114.8.35          0 18508 ?
*>  4.0.0.0/8        63.114.8.33          0 18508 701 1 i
*>  4.2.49.12/30     63.114.8.33          0 18508 209 i
*   4.17.250.0/24    63.114.8.33          0 18508 209 1239 13716 i
*>  63.114.8.33      63.114.8.33          0 18508 701 1239 13716 i
*   4.21.132.0/23    63.114.8.33          0 18508 209 6461 16422 i
*>  4.21.132.0/23    63.114.8.33          0 18508 701 6461 16422 i
*>  4.24.118.16/30   63.114.8.33          0 18508 209 i
*>  4.24.145.0/30    63.114.8.33          0 18508 209 i
*>  4.24.187.12/30   63.114.8.33          0 18508 209 i
*>  4.24.202.0/30    63.114.8.33          0 18508 209 i
*>  4.25.88.0/30     63.114.8.33          0 18508 209 3561 3908 i
*>  5.0.0.0/9        63.114.8.33          0 18508 ?
*>  5.0.0.0/10       63.114.8.33          0 18508 ?
*>  5.0.0.0/11       63.114.8.33          0 18508 ?
--More--
```

Following is the example for displaying all the received routes from all IPv4 neighbors:

```
DelleMC# show ip bgp vrf test ipv4 unicast neighbors all received-routes
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 1.1.1.1
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
ID 110.1.1.0/24     11.1.1.2          0          100     0 ?
*>I 111.1.1.0/24    11.1.1.2          0          100     0 ?
ID 112.1.1.0/24     11.1.1.2          0          100     0 ?
*>I 113.1.1.0/24    11.1.1.2          0          100     0 ?
ID 114.1.1.0/24     11.1.1.2          0          100     0 ?
*>I 115.1.1.0/24    11.1.1.2          0          100     0 ?
ID 116.1.1.0/24     11.1.1.2          0          100     0 ?
ID 117.1.1.0/24     11.1.1.2          0          100     0 ?
ID 118.1.1.0/24     11.1.1.2          0          100     0 ?
ID 119.1.1.0/24     11.1.1.2          0          100     0 ?
ID 120.1.1.0/24     11.1.1.2          0          100     0 ?
```

Following is the example for displaying all the received routes from all IPv6 neighbors:

```
DelleMC# show ip bgp ipv6 unicast neighbors all received-routes
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 11.1.1.1
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 200::/64                 12::2                    0           0  i
*>I 200:0:0:1::/64          12::2                    0           0  i
*>I 200:0:0:2::/64          12::2                    0           0  i
*>I 200:0:0:3::/64          12::2                    0           0  i
*>I 200:0:0:4::/64          12::2                    0           0  i
*>I 200:0:0:5::/64          12::2                    0           0  i
*>I 200:0:0:6::/64          12::2                    0           0  i
*>I 200:0:0:7::/64          12::2                    0           0  i
*>I 200:0:0:8::/64          12::2                    0           0  i
*>I 200:0:0:9::/64          12::2                    0           0  i
*>I 200:0:0:a::/64          12::2                    0           0  i
*>I 200:0:0:b::/64          12::2                    0           0  i
*>I 200:0:0:c::/64          12::2                    0           0  i
*>I 200:0:0:d::/64          12::2                    0           0  i
*>I 200:0:0:e::/64          12::2                    0           0  i
*>I 200:0:0:f::/64          12::2                    0           0  i
*>I 200:0:0:10::/64         12::2                    0           0  i
*>I 200:0:0:11::/64         12::2                    0           0  i
*>I 200:0:0:12::/64         12::2                    0           0  i
*>I 200:0:0:13::/64         12::2                    0           0  i
```

### 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 [ipv4 unicast] cluster-list [cluster-id]`

**Parameters**

***ipv4 unicast*** (OPTIONAL) Enter the keywords *ipv4 unicast* to view information only related to *ipv4 unicast* routes.

***cluster-id*** (OPTIONAL) Enter the cluster id in dotted decimal format. The range is 1 — 4294967295.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip bgp cluster-list` command shown in the following example.

Field	Description
<b>Network</b>	Displays the destination network prefix of each BGP route.

Field	Description
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	Lists all the ASs the route passed through to reach the destination network.

### Example

```
Dell#show ip bgp cluster-list
BGP table version is 64444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n
- network
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop      Metric LocPrf Weight Path
* I 10.10.10.1/32      192.68.16.1    0     100     0 i
* I                    192.68.16.1    0     100     0 i
*>I                    192.68.16.1    0     100     0 i
* I                    192.68.16.1    0     100     0 i
* I                    192.68.16.1    0     100     0 i
* I                    192.68.16.1    0     100     0 i
* I 10.19.75.5/32     192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
*>I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
* I 10.30.1.0/24      192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
*>I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
* I                    192.68.16.1    0     100     0 ?
```

## show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

**Syntax** `show ip bgp [ipv4 unicast] community [community-number] [local-as] [no-export] [no-advertise]`

Parameters	Description
<b>ipv4 unicast</b>	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
<b>community-number</b>	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.
<b>local-AS</b>	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 (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
<b>no-advertise</b>	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 (0xFFFFFFFF02) 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 (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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
<b>Network</b>	Displays the destination network prefix of each BGP route.
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	Lists all the ASs the route passed through to reach the destination network.

**Example**

```
Dell>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop      Metric LocPrf Weight Path
* i 3.0.0.0/8     205.171.0.16 100    0 209 701 80 i
*>i 4.2.49.12/30  205.171.0.16 100    0 209 i
* i 4.21.132.0/23 205.171.0.16 100    0 209 6461 16422 i
*>i 4.24.118.16/3 205.171.0.16 100    0 209 i
*>i 4.24.145.0/30 205.171.0.16 100    0 209 i
*>i 4.24.187.12/30 205.171.0.16 100    0 209 i
*>i 4.24.202.0/30 205.171.0.16 100    0 209 i
*>i 4.25.88.0/30  205.171.0.16 100    0 209 3561 3908 i
*>i 6.1.0.0/16    205.171.0.16 100    0 209 7170 1455 i
*>i 6.2.0.0/22    205.171.0.16 100    0 209 7170 1455 i
*>i 6.3.0.0/18    205.171.0.16 100    0 209 7170 1455 i
*>i 6.4.0.0/16    205.171.0.16 100    0 209 7170 1455 i
*>i 6.5.0.0/19    205.171.0.16 100    0 209 7170 1455 i
*>i 6.8.0.0/20    205.171.0.16 100    0 209 7170 1455 i
*>i 6.9.0.0/20    205.171.0.16 100    0 209 7170 1455 i
*>i 6.10.0.0/15   205.171.0.16 100    0 209 7170 1455 i
*>i 6.14.0.0/15   205.171.0.16 100    0 209 7170 1455 i
*>i 6.133.0.0/21  205.171.0.16 100    0 209 7170 1455 i
```

```
*>i 6.151.0.0/1      205.171.0.16      100      0 209 7170 1455 i
--More--
```

## show ip bgp community-list

View routes that a specific community list affects.

**Syntax** `show ip bgp [ipv4 unicast] community-list community-list-name [exact-match]`

**Parameters**

**ipv4 unicast** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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
<b>Network</b>	Displays the destination network prefix of each BGP route.
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	Lists all the ASs the route passed through to reach the destination network.

**Example**

```
Dell#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

Network      Next Hop      Metric      LocPrf      Weight Path
Dell#
```

# show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

**Syntax** `show ip bgp [ipv4 unicast] dampened-paths`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
<b>Network</b>	Displays the network ID to which the route is dampened.
<b>From</b>	Displays the IP address of the neighbor advertising the dampened route.
<b>Reuse</b>	Displays the hour:minutes:seconds until the dampened route is available.
<b>Path</b>	Lists all the ASs the dampened route passed through to reach the destination network.

## Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      From      Reuse      Path
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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics
74857 :
NhLocAS 1 : NdState 2 : NdRPMPprim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal
```

```

-1 :
NdIgnrIlliId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0
:
NdRRClstTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP
0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRC1P 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 : Fatals 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d4 :
RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP 0x41a1b750 :
TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 :
LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 :
AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 : CleanRibTmrP
0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP
0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : EnforcelstAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpcioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 : NonDet 0 :
DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 : IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaxeorExtInt
361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP 0x41a19d28 :
NdRTMAFTblVer 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPprefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 :
NdAFWPtR 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.

<b>Syntax</b>	<code>show ip bgp [<i>ipv4 unicast</i>] extcommunity-list [<i>list name</i>]</code>	
<b>Parameters</b>	<b><i>ipv4 unicast</i></b>	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
	<b><i>list name</i></b>	Enter the extended community list name you wish to view. The range is 140 characters.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	To view the total number of COMMUNITY attributes found, use the <code>show ip bgp summary</code> command. The text line above the route table states the number of COMMUNITY attributes found.  The <code>show ip bgp community</code> command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the <code>show ip bgp</code> command output.	

## show ip bgp filter-list

View the routes that match the filter lists.

<b>Syntax</b>	<code>show ip bgp [<i>ipv4 unicast</i>] filter-list <i>as-path-name</i></code>	
<b>Parameters</b>	<b><i>ipv4 unicast</i></b>	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
	<b><i>as-path-name</i></b>	Enter an AS-PATH access list name. The range is 140 characters.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	The following describes the <code>show ip bgp filter-list hello</code> command shown in the following example.	
	<b>Field</b>	<b>Description</b>
	<b>Path source codes</b>	Lists the path sources shown to the right of the last AS number in the Path column:

Field	Description
	<ul style="list-style-type: none"> <li>• i = internal route entry</li> <li>• a = aggregate route entry</li> <li>• c = external confederation route entry</li> <li>• n = network route entry</li> <li>• r = redistributed route entry</li> </ul>
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	Lists all the ASs the route passed through to reach the destination network.

### Example

```
Dell#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n -
network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network      Next Hop                Metric LocPrf Weight Path
* I 6.1.5.0/24  192.100.11.2            20000   9999    0 ?
* I              192.100.8.2             20000   9999    0 ?
* I              192.100.9.2             20000   9999    0 ?
* I              192.100.10.2            20000   9999    0 ?
*>I             6.1.5.1                  20000   9999    0 ?
* I             6.1.6.1                   20000   9999    0 ?
* I             6.1.20.1                  20000   9999    0 ?
* I             6.1.6.0/24 192.100.11.2        20000   9999    0 ?
* I             192.100.8.2              20000   9999    0 ?
* I             192.100.9.2              20000   9999    0 ?
* I             192.100.10.2             20000   9999    0 ?
*>I             6.1.5.1                  20000   9999    0 ?
* I             6.1.6.1                   20000   9999    0 ?
* I             6.1.20.1                  20000   9999    0 ?
* I             6.1.20.0/24 192.100.11.2        20000   9999    0 ?
* I             192.100.8.2              20000   9999    0 ?
* I             192.100.9.2              20000   9999    0 ?
* I             192.100.10.2             20000   9999    0 ?
Dell#
```

## show ip bgp flap-statistics


View flap statistics on BGP routes.

**Syntax** `show ip bgp [ipv4 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regex regular-expression]`

Parameters	Description
<b><i>ipv4 unicast</i></b>	(OPTIONAL) Enter the keywords <i>ipv4 unicast</i> to view information only related to <i>ipv4 unicast</i> routes.
<b><i>ip-address</i></b>	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
<b><i>mask</i></b>	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
<b><i>filter-list as-path-name</i></b>	(OPTIONAL) Enter the keyword <i>filter-list</i> then the name of a configured AS-PATH ACL. The range is 140 characters.

### regex *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

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

The following describes the `show ip bgp flap` command shown in the following example.

Field	Description
<b>Network</b>	Displays the network ID to which the route is flapping.
<b>From</b>	Displays the IP address of the neighbor advertising the flapping route.
<b>Flaps</b>	Displays the number of times the route flapped.
<b>Duration</b>	Displays the hours:minutes:seconds since the route first flapped.
<b>Reuse</b>	Displays the hours:minutes:seconds until the flapped route is available.
<b>Path</b>	Lists all the ASs the flapping route passed through to reach the destination network.

#### Example

```
Dell>show ip bgp flap-statistics
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external,
              r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network      From      Flaps      Duration      Reuse      Path
Dell>
```

## 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 [ipv4 unicast] inconsistent-as`

- Command Modes**
- EXEC

- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip bgp inconsistent-as` command shown in the following example.

Field	Description
<b>Network</b>	Displays the destination network prefix of each BGP route.
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP route's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight.
<b>Path</b>	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 18508 ?
*               63.114.8.33              0 18508 209 3549 i
*   9.2.0.0/16   63.114.8.60              0 18508 209 701 i
*               63.114.8.34              0 18508 209 701 i
--More--
```

## show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.


**Syntax**

```
show ip bgp [ipv4 unicast] neighbors [ip-address [advertised-routes |
dampened-routes | detail | flap-statistics | routes | {received-routes
[network [network-mask]]} | {denied-routes [network [network-mask]]}]
```

**Parameters**

**ipv4 unicast** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.



<b><i>ip-address</i></b>	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
<b>advertised-routes</b>	(OPTIONAL) Enter the keywords <code>advertised-routes</code> to view only the routes the neighbor sent.
<b>dampened-routes</b>	(OPTIONAL) Enter the keywords <code>dampened-routes</code> to view information on dampened routes from the BGP neighbor.
<b>detail</b>	(OPTIONAL) Enter the keyword <code>detail</code> to view neighbor-specific internal information for the IPv4 Unicast address family.
<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to view flap statistics on the neighbor's routes.
<b>routes</b>	(OPTIONAL) Enter the keyword <code>routes</code> to view only the neighbor's feasible routes.
<b>received-routes</b> <b>[<i>network</i>]</b> <b>[<i>network-mask</i>]</b>	(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.  <b>NOTE:</b> Configure the <code>neighbor soft-reconfiguration inbound</code> command prior to viewing all the information received from the neighbors.
<b>denied-routes</b> <b>[<i>network</i>]</b> <b>[<i>network-mask</i>]</b>	(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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

After a peer reset, the contents of the notification log messages is displayed in hex values for debugging. The following describes the `show ip bgp neighbors` command shown in the following examples.

The Lines Beginning with:	Description
<b>BGP neighbor</b>	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.
<b>BGP version</b>	Displays the BGP version (always version 4) and the remote router ID.
<b>BGP state</b>	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
<b>Last read</b>	This line displays the following information: <ul style="list-style-type: none"> <li>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</li> <li>• hold time is the number of seconds configured between messages from its neighbor</li> <li>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</li> </ul>
<b>Received messages</b>	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.

The Lines Beginning with:	Description
<b>Sent messages</b>	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.
<b>Received updates</b>	This line displays the number of BGP updates received and sent.
<b>Soft reconfiguration</b>	This line indicates that soft reconfiguration inbound is configured.
<b>Minimum time</b>	Displays the minimum time, in seconds, between advertisements.
<b>(list of inbound and outbound policies)</b>	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
<b>For address family:</b>	Displays the IPv4 Unicast as the address family.
<b>BGP table version</b>	Displays which version of the primary BGP routing table the router and the neighbor are using.
<b>accepted prefixes</b>	Displays the number of network prefixes the router accepts and the amount of memory used to process those prefixes.
<b>Prefix advertised</b>	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
<b>Connections established</b>	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
<b>Last reset</b>	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.
<b>Local host:</b>	Displays the peering address of the local router and the TCP port number.
<b>Foreign host:</b>	Displays the peering address of the neighbor and the TCP port number.

#### Example ( )

```
Dell#show ip bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 23456, external link
  BGP version 4, remote router ID 10.10.10.1
  BGP state ESTABLISHED, in this state for 00:00:35
. . .
  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    4_OCTECT_AS(65)
    ADD_PATH_(69)
    CISCO_ROUTE_REFRESH(128)
```

#### Example

```
Dell#show ip bgp neighbors
BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
  3 opens, 1 notifications, 1394 updates
  6 keepalives, 0 route refresh requests
Sent 48 messages, 0 in queue
  3 opens, 2 notifications, 0 updates
  43 keepalives, 0 route refresh requests
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)
CISCO_ROUTE_REFRESH(128)
```

Capabilities advertised to neighbor for IPv4 Unicast :

```
MULTIPROTO_EXT(1)
ROUTE_REFRESH(2)
ROUTE_REFRESH(2)
GRACEFUL_RESTART(64)
CISCO_ROUTE_REFRESH(128)
```

Route map for incoming advertisements is test  
Maximum prefix set to 4 with threshold 75

For address family: IPv4 Unicast  
BGP table version 34, neighbor version 34  
5 accepted prefixes consume 20 bytes  
Prefix advertised 0, denied 4, withdrawn 0

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer  
Prefixes advertised 0, rejected 0, withdrawn 0 from peer

Connections established 2; dropped 1  
Last reset 00:18:21, due to Maximum prefix limit reached

### Example (Advertised- Routes)

```
Dell>show ip bgp neighbors 192.14.1.5 advertised-routes
```

BGP table version is 74103, local router ID is 33.33.33.33  
Status codes: s suppressed, S stale, d damped, h history, \* valid, > best  
Path source: I - internal, a - aggregate, c - confed-external, r -  
redistributed,  
n - network  
Origin codes: i - IGP, e - EGP, ? - incomplete

	Network	Next	Hop	Metric	LocPrf	Weight	Path
*>r	1.10.1.0/24		0.0.0.0	5000		32768	?
*>r	1.11.0.0/16		0.0.0.0	5000		32768	?
.....							
...							
*>I	223.94.249.0/24	223.100.4.249		0	100		0 ?
*>I	223.94.250.0/24	223.100.4.250		0	100		0 ?
*>I	223.100.0.0/16	223.100.255.254		0	100		0 ?

Total number of prefixes: 74102

### Example (Received- Routes)

BGP table version is 13, local router ID is 120.10.10.1  
Status codes: s suppressed, S stale, d damped, 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
D	70.70.21.0/24	100.10.10.2		0	0 100 200	?
D	70.70.22.0/24	100.10.10.2		0	0 100 200	?
D	70.70.23.0/24	100.10.10.2		0	0 100 200	?
D	70.70.24.0/24	100.10.10.2		0	0 100 200	?
*>	70.70.25.0/24	100.10.10.2		0	0 100 200	?
*>	70.70.26.0/24	100.10.10.2	0	0	0 100 200	?
*>	70.70.27.0/24	100.10.10.2	0	0	0 100 200	?
*>	70.70.28.0/24	100.10.10.2	0	0	0 100 200	?
*>	70.70.29.0/24	100.10.10.2	0	0	0 100 200	?

Dell#

### Example (denied- routes)

```
Dell#show ip bgp neighbors 100.10.10.2 denied-routes
```

4 denied paths using 205 bytes of memory  
BGP table version is 34, local router ID is 100.10.10.2  
Status codes: s suppressed, S stale, d damped, 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
D  70.70.21.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.22.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.23.0/24    100.10.10.2              0      0 100 200 ?
D  70.70.24.0/24    100.10.10.2              0      0 100 200 ?
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 next-hop`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip bgp next-hop` command shown in the following example.

Field	Description
<b>Next-hop</b>	Displays the next-hop IP address.
<b>Via</b>	Displays the IP address and interface used to reach the next hop.
<b>RefCount</b>	Displays the number of BGP routes using this next hop.
<b>Cost</b>	Displays the cost associated with using this next hop.
<b>Flaps</b>	Displays the number of times the next hop has flapped.
<b>Time Elapsed</b>	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      Via                               RefCount Cost Flaps Time Elapsed
 63.114.8.33    63.114.8.33, Gi 12/22           240984   0    0 00:18:25
 63.114.8.34    63.114.8.34, Gi 12/22           135152   0    0 00:18:13
 63.114.8.35    63.114.8.35, Gi 12/22             1    0    0 00:18:07
 63.114.8.60    63.114.8.60, Gi 12/22           135155   0    0 00:18:11
Dell>

```

## show ip bgp paths

View all the BGP path attributes in the BGP database.

**Syntax** `show ip bgp paths [regex regular-expression]`

## Parameters

### **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).
- **i** **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

**Supported Modes** Full-Switch

### **Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### **Usage Information**

The following describes the `show ip bgp path` command shown in the following example.

<b>Field</b>	<b>Description</b>
<b>Total</b>	Displays the total number of BGP path attributes.
<b>Address</b>	Displays the internal address where the path attribute is stored.
<b>Hash</b>	Displays the hash bucket where the path attribute is stored.
<b>Refcount</b>	Displays the number of BGP routes using this path attribute.
<b>Metric</b>	Displays the MED attribute for this path attribute.
<b>Path</b>	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

### **Example**

```
Dell#show ip bgp path
Total 16 Paths
Address      Hash Refcount  Metric Path
0x1efe7e5c   15      10000         32 ?
0x1efe7e1c   71      10000         23 ?
0x1efe7ddc   127     10000         22 ?
0x1efe7d9c   183     10000         43 ?
0x1efe7d5c   239     10000         42 ?
0x1efe7c9c   283          6         {102 103} ?
0x1efe7b1c   287     336 20000         ?
0x1efe7d1c   295     10000         13 ?
0x1efe7c5c   339          6         {92 93} ?
0x1efe7cdc   351     10000         12 ?
0x1efe7c1c   395          6         {82 83} ?
0x1efe7bdc   451          6         {72 73} ?
0x1efe7b5c   491         78          0 ?
0x1efe7adc   883          2         120 i
0x1efe7e9c   983     10000         33 ?
0x1efe7b9c  1003          6          0 i
Dell#
```

# show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

**Syntax** `show ip bgp paths as-path`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip bgp paths as-path` command shown in the following example.

Field	Description
<b>Address</b>	Displays the internal address where the path attribute is stored.
<b>Hash</b>	Displays the hash bucket where the path attribute is stored.
<b>Refcount</b>	Displays the number of BGP routes using these AS-Paths.
<b>AS-Path</b>	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

## Example

```
Dell#show ip bgp paths as-path
Total 13 AS-Paths
Address      Hash  Refcount  AS-Path
0x1ea3c1ec   251      1      42
0x1ea3c25c   251      1      22
0x1ea3c1b4   507      1      13
0x1ea3c304   507      1      33
0x1ea3c10c   763      1      {92 93}
0x1ea3c144   763      1      {102 103}
0x1ea3c17c   763      1      12
0x1ea3c2cc   763      1      32
0x1ea3c09c   764      1      {72 73}
0x1ea3c0d4   764      1      {82 83}
0x1ea3c224   1019     1      43
0x1ea3c294   1019     1      23
0x1ea3c02c   1021     4
Dell#
```

# show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

**Syntax** `show ip bgp paths community`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show ip bgp paths community` command shown in the following example.

Field	Description
<b>Address</b>	Displays the internal address where the path attribute is stored.
<b>Hash</b>	Displays the hash bucket where the path attribute is stored.
<b>Refcount</b>	Displays the number of BGP routes using these communities.
<b>Community</b>	Displays the community attributes in this BGP path.

## Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address      Hash    Refcount Community
0x1ec88a5c   3       4 209:209 209:6059 209:31272 3908:900
19092:300
0x1e0f10ec   15      4 209:209 209:3039 209:31272 3908:900
19092:300
0x1c902234   37      2 209:209 209:7193 209:21362 3908:900
19092:300
0x1f588cd4   41      24 209:209 209:6253 209:21362 3908:900
19092:300
0x1e805884   46      2 209:209 209:21226 286:777 286:3033 1899:3033
64675:21092
0x1e433f4c   46      8 209:209 209:5097 209:21362 3908:900
19092:300
0x1f173294   48      16 209:209 209:21226 286:40 286:777 286:3040
5606:40
12955:5606
0x1c9f8e24   50      6 209:209 209:4069 209:21362 3908:900
19092:300
0x1c9f88e4   53      4 209:209 209:3193 209:21362 3908:900
19092:300
0x1f58a944   57      6 209:209 209:2073 209:21362 3908:900
19092:300
0x1ce6be44   80      2 209:209 209:999 209:40832
0x1c6e2374   80      2 209:777 209:41528
0x1f58ad6c   82      46 209:209 209:41528
0x1c6e2064   83      2 209:777 209:40832
0x1f588ecc   85      570 209:209 209:40832
0x1f57cc0c   98      2 209:209 209:21226 286:3031 13646:1044
13646:1124
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204 13646:1214
13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac   117     6 209:209 209:999 209:31272
0x1f5854ac   119     18 209:209 209:21226 286:108 286:111 286:777
286:3033
517:5104
```

## show ip bgp peer-group

Allows you to view information on the BGP peers in a peer group.

**Syntax** `show ip bgp [ipv4 unicast] peer-group [peer-group-name [detail | summary]]`

**Parameters**

- ipv4 unicast** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
- peer-group-name** (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
- detail** (OPTIONAL) Enter the keyword `detail` to view detailed status information of the peers in that peer group.

**summary** (OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp summary` command.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip bgp peer-group` command shown in the following example.

**Line beginning with:**

<b>Peer-group</b>	Displays the peer group's name.
<b>Administratively shut</b>	Displays the peer group's status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
<b>BGP version</b>	Displays the BGP version supported.
<b>Minimum time</b>	Displays the time interval between BGP advertisements.
<b>For address family</b>	Displays IPv4 Unicast as the address family.
<b>BGP neighbor</b>	Displays the name of the BGP neighbor.
<b>Number of peers</b>	Displays the number of peers currently configured for this peer group.
<b>Peer-group members:</b>	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

**Example ( )**

```
Dell#show ip bgp peer-group

Peer-group pgl
  BGP version 4
  Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
  BGP neighbor is pgl
Number of peers in this group 4
Update packing has 4_OCTECT_AS support enabled
Add-path support enabled
Peer-group members (* - outbound optimized):
  1.1.1.5
  1.1.1.6
  10.10.10.2*
  20.20.20.100
```

**Example**

```
Dell#show ip bgp peer-group

Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
```



```

12.1.1.3*
12.1.1.4*
12.1.1.5*
12.1.1.6*
12.2.1.2*
12.2.1.3*
12.2.1.4*
12.2.1.5*
12.2.1.6*
12.3.1.2*
12.3.1.3*
12.3.1.4*
12.3.1.5*
12.3.1.6*
12.4.1.2*
12.4.1.3*
12.4.1.4*
12.4.1.5*
12.4.1.6*

```

### 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 table matching the regular expressions specified.

**Syntax** `show ip bgp regexp regular-expression [character]`

### Parameters

***regular-expression***  
**[*character*]**

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
  - `*` = (asterisk) the sequences in a pattern (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

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip bgp regexp` command shown in the following example.

Field	Description
<b>Network</b>	Displays the destination network prefix of each BGP route.

Field	Description
<b>Next Hop</b>	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.
<b>Metric</b>	Displays the BGP router's metric, if assigned.
<b>LocPrf</b>	Displays the BGP LOCAL_PREF attribute for the route.
<b>Weight</b>	Displays the route's weight
<b>Path</b>	Lists all the AS paths the route passed through to reach the destination network.

### Example (S4810)

```
Dell#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network      Next Hop      Metric LocPrf Weight Path
*>I 3.0.0.0/8      1.1.1.2        0 100      0 2914 1239 80 i
*>I 4.0.0.0/8      1.1.1.2        0 100      0 2914 3356 i
*>I 4.17.225.0/24  1.1.1.2        0 100      0 2914 11853 11853 11853
11853 11853 6496
*>I 4.17.226.0/23  1.1.1.2        0 100      0 2914 11853 11853 11853
11853 11853 6496
*>I 4.17.251.0/24  1.1.1.2        0 100      0 2914 11853 11853 11853
11853 11853 6496
*>I 4.17.252.0/23  1.1.1.2        0 100      0 2914 11853 11853 11853
11853 11853 6496
*>I 4.19.2.0/23    1.1.1.2        0 100      0 2914 701 6167 6167
6167 i
*>I 4.19.16.0/23   1.1.1.2        0 100      0 2914 701 6167 6167
6167 i
*>I 4.21.80.0/22   1.1.1.2        0 100      0 2914 174 4200 16559 i
*>I 4.21.82.0/24   1.1.1.2        0 100      0 2914 174 4200 16559 i
*>I 4.21.252.0/23  1.1.1.2        0 100      0 2914 701 6389 8063
19198 i
*>I 4.23.180.0/24  1.1.1.2        0 100      0 2914 3561 6128 30576 i
*>I 4.36.200.0/21  1.1.1.2        0 100      0 2914 14742 11854 14135
i
*>I 4.67.64.0/22   1.1.1.2        0 100      0 2914 11608 19281 i
*>I 4.78.32.0/21   1.1.1.2        0 100      0 2914 3491 29748 i
*>I 6.1.0.0/16      1.1.1.2        0 100      0 2914 701 668 i
*>I 6.2.0.0/22      1.1.1.2        0 100      0 2914 701 668 i
*>I 6.3.0.0/18      1.1.1.2        0 100      0 2914 701 668 i
```

## show ip bgp summary

Allows you to view the status of all BGP connections.

**Syntax** `show ip bgp [ipv4 unicast] summary`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip bgp summary` command shown in the following example.

Field	Description								
<b>BGP router identifier</b>	Displays the local router ID and the AS number.								
<b>BGP table version</b>	Displays the BGP table version and the main routing table version.								
<b>network entries</b>	Displays the number of network entries, route paths, and the amount of memory used to process those entries.								
<b>paths</b>	Displays the number of paths and the amount of memory used.								
<b>denied paths</b>	Displays the number of denied paths and the amount of memory used.								
<b>BGP path attribute entries</b>	Displays the number of BGP path attributes and the amount of memory used to process them.								
<b>BGP AS-PATH entries</b>	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.								
<b>BGP community entries</b>	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.								
<b>Dampening enabled</b>	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.								
<b>Neighbor</b>	Displays the BGP neighbor address.								
<b>AS</b>	Displays the AS number of the neighbor.								
<b>MsgRcvd</b>	Displays the number of BGP messages that neighbor received.								
<b>MsgSent</b>	Displays the number of BGP messages that neighbor sent.								
<b>TblVer</b>	Displays the version of the BGP table that was sent to that neighbor.								
<b>InQ</b>	Displays the number of messages from that neighbor waiting to be processed.								
<b>OutQ</b>	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.								
<b>Up/Down</b>	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 <code>never</code> is displayed. The output format is: <table border="1" data-bbox="571 1375 1040 1585"> <thead> <tr> <th>Time</th> <th>Display Example</th> </tr> </thead> <tbody> <tr> <td><b>&lt; 1 day</b></td> <td>00:12:23 (hours:minutes:seconds)</td> </tr> <tr> <td><b>&lt; 1 week</b></td> <td>1d21h (DaysHours)</td> </tr> <tr> <td><b>&gt; 1 week</b></td> <td>11w2d (WeeksDays)</td> </tr> </tbody> </table>	Time	Display Example	<b>&lt; 1 day</b>	00:12:23 (hours:minutes:seconds)	<b>&lt; 1 week</b>	1d21h (DaysHours)	<b>&gt; 1 week</b>	11w2d (WeeksDays)
Time	Display Example								
<b>&lt; 1 day</b>	00:12:23 (hours:minutes:seconds)								
<b>&lt; 1 week</b>	1d21h (DaysHours)								
<b>&gt; 1 week</b>	11w2d (WeeksDays)								
<b>State/Pfxrcd</b>	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 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 (S4810)

```
Dell#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
```

```

BGP table version is 34, main routing table version 34
9 network entrie(s) using 1372 bytes of memory
5 paths using 380 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entrie(s) using 168 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
1 BGP community entrie(s) using 43 bytes of memory
2 neighbor(s) using 7232 bytes of memory

Neighbor  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/Pfx
100.10.10.2 200    46       41       34     0    0  00:14:33    5
120.10.10.2 300    40       47       34     0    0  00:37:10    0
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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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		
<b><i>keepalive</i></b>	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 <b>60 seconds</b> .	
<b><i>holdtime</i></b>	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 <b>180 seconds</b> .	

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# timers bgp extended

Adjust the BGP idle holdtime for all the BGP neighbors.

<b>Syntax</b>	<code>timers bgp extended idle-holdtime</code> To return to the default, use the <code>no timers bgp extended</code> command.				
<b>Parameters</b>	<b>extended idle-holdtime</b> Enter a number for the time interval, in seconds, for the peer to be idle state. The range is from 1 to 32767. The default is <b>15 seconds</b> .				
<b>Defaults</b>	The default <i>idle-holdtime</i> is <b>15 seconds</b> .				
<b>Command Modes</b>	EXEC Privilege				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .				
	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.14(0.0)</b></td><td>Introduced on the C9010, MXL, FN IOM, S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, Z9500, and S6000-ON.</td></tr></tbody></table>	Version	Description	<b>9.14(0.0)</b>	Introduced on the C9010, MXL, FN IOM, S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, Z9500, and S6000-ON.
Version	Description				
<b>9.14(0.0)</b>	Introduced on the C9010, MXL, FN IOM, S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, Z9500, and S6000-ON.				
<b>Usage Information</b>	The peer remains in idle state based on the configured <i>idle-holdtime</i> . The less the <i>idle-holdtime</i> , lesser the peer in idle state.  For the new <i>idle-holdtime</i> to take effect, you need to shutdown all the peers manually using <code>neighbor shutdown</code> command and enable the peers again.				

## MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs).

MBGP is implemented as per IETF RFC 1858.

## debug ip bgp dampening

View information on routes being dampened.

<b>Syntax</b>	<code>debug ip bgp ipv4 multicast dampening</code> To disable debugging, use the <code>no debug ip bgp ipv4 multicast dampening</code> command.						
<b>Parameters</b>	<b>dampening</b> Enter the keyword <i>dampening</i> to clear route flap dampening information.						
<b>Command Modes</b>	EXEC Privilege						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

## 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**

- external-distance** Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.
- internal-distance** Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
- local-distance** Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

**Defaults**

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**


**Command Modes** ROUTER BGP (conf-router\_bgp\_af)

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

 **CAUTION: Dell Networking OS 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 [ipv4 unicast] dampened-paths`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
<b>Network</b>	Displays the network ID to which the route is dampened.
<b>From</b>	Displays the IP address of the neighbor advertising the dampened route.
<b>Reuse</b>	Displays the hour:minutes:seconds until the dampened route is available.

Field	Description
Path	Lists all the ASs the dampened route passed through to reach the destination network.

### Example

```
Dell>show ip bgp dampened-paths
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network      From      Reuse      Path
Dell>
```

## BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute.

BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

### set extcommunity rt

To set Route Origin community attributes in Route Map, use this feature.

**Syntax** `set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]`

To delete the Route Origin community, use the `no set extcommunity` command.

Parameters		
<b>as4 ASN4:NN</b>	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).	
<b>ASN:NNNN</b>	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).	
<b>IPADDR:NN</b>	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).	
<b>additive</b>	(OPTIONAL) Enter the keyword <code>additive</code> to add to the existing extended community.	
<b>non-trans</b>	(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.	

**Defaults** none

**Command Modes** ROUTE MAP (config-route-map)

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If the `set community rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.

- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

**Related Commands**

[set extcommunity soo](#) — sets the extended community site-of-origin in the route-map.

## set extcommunity soo

To set extended community site-of-origin in Route Map, use this feature.

**Syntax** `set extcommunity soo {as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]}`  
 To delete the site-of-origin community, use the `no set extcommunity` command.

**Parameters**

<b>as4 ASN4:NN</b>	Enter the keyword <code>as4</code> then the 4-octet AS specific extended community number in the format <code>ASN4:NN</code> (4-byte AS number:2-byte community value).
<b>ASN:NNNN</b>	Enter the 2-octet AS specific extended community number in the format <code>ASN:NNNN</code> (2-byte AS number:4-byte community value).
<b>IPADDR:NN</b>	Enter the IP address specific extended community in the format <code>IPADDR:NN</code> (4-byte IPv4 Unicast Address:2-byte community value).
<b>non-trans</b>	(OPTIONAL) Enter the keywords <code>non-trans</code> to indicate a non-transitive BGP extended community.

**Defaults** none

**Command Modes** ROUTE MAP (config-route-map)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If the `set community rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

**Related Commands**

[set extcommunity rt](#) — sets the extended community route origins using the route-map.

## show ip bgp paths extcommunity

To display all BGP paths having extended community attributes, use this feature.

**Syntax** `show ip bgp paths extcommunity`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

The following describes the `show ip bgp paths extcommunity` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

#### Example

```
Dell#show ip bgp paths extcommunity
Total 1 Extended Communities

Address      Hash  Refcount  Extended Community
0x41d57024  12272  1         RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

Dell#
```

## show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

**Syntax** `show ip bgp [ipv4 unicast] extcommunity-list [list name]`

**Parameters**

- ipv4 unicast*** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to `ipv4 unicast` routes.
- list name*** Enter the extended community list name you wish to view. The range is 140 characters.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

## IPv6 BGP Commands

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on the switch.

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 interdomain routing 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.

# bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

**Syntax** `bgp soft-reconfig-backup`  
To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults** Disabled

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

**Related Commands** `clear ip bgp` — activates inbound policies without resetting the BGP TCP session.

# clear ip bgp ipv6 unicast soft

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.

**Syntax** `clear ip bgp { * | as-number | ipv4-neighbor-addr | ipv6-neighbor-addr | peer-group name } ipv6 unicast soft [ in | out ]`

Parameters	Description
<b>*</b>	Clear and reapply an asterisk ( * ) for all BGP sessions.
<b>as-number</b>	Clear and reapply policies for all neighbors belonging to the AS. The range is from 0 to 65535 (2 Byte), from 1 to 4294967295 (4 Byte), or from 0.1 to 0.65535.65535 (Dotted format).
<b>ipv4-neighbor-addr   ipv6-neighbor-addr</b>	Clear and reapply policies for a neighbor.
<b>peer-group name</b>	Clear and reapply policies for all BGP routers in the specified peer group.
<b>ipv6 unicast soft</b>	Clear and reapply policies for all IPv6 unicast routes.
<b>in</b>	Reapply only inbound policies. <b>NOTE:</b> If you enter <code>soft</code> , without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.
<b>out</b>	Reapply only outbound policies. <b>NOTE:</b> If you enter <code>soft</code> , without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

**Syntax** `debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration`

To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration` command.

**Parameters**

- ipv4-address* | *ipv6-address*** Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
- peer-group-name*** Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
- ipv6 unicast** Debug soft reconfiguration for IPv6 unicast routes.

**Defaults** Disabled.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

## ipv6 prefix-list

Configure an IPv6 prefix list.

**Syntax** `ipv6 prefix-list prefix-list name`

**Parameters**

- prefix-list name*** Enter the name of the prefix list.  
 **NOTE:** There is a 140-character limit for prefix list names.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.


**Related Commands** [show ipv6 prefix-list](#) — View the selected IPv6 prefix-list.

# show ipv6 prefix-list

Displays the specified IPv6 prefix list.

**Syntax** `show ipv6 prefix-list detail {prefix-list name} | summary`

**Parameters**

<b>detail</b>	Display a detailed description of the selected IPv6 prefix list.
<b><i>prefix-list name</i></b>	Enter the name of the prefix list.  <b>NOTE:</b> There is a 140-character limit for prefix list names.
<b>summary</b>	Display a summary of RPF routes.

**Command Modes** EXEC

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Command History** **Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [ipv6 prefix-list](#) — configures an IPv6 prefix-list.

## IPv6 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 (AS).


MBGP is implemented as per IETF RFC 1858.

# show ipv6 mbgproutes

Display the selected IPv6 MBGP route or a summary of all MBGP routes in the table.

**Syntax** `show ipv6 mbgproutes ipv6-address prefix-length | summary`

**Parameters**

<b><i>ipv6-address</i></b>	(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.
<b><i>prefix-length</i></b>	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>summary</b>	Display a summary of RPF routes.

**Command Modes** EXEC

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# Configuration Cloning

Configuration Cloning enables you to clone the configuration from one aggregator to the other. It identifies a source aggregator where running configuration is check-pointed, extracted and downloaded to the target aggregator for further use. The target aggregator checks the compatibility of the cloning file regarding the mode, port types and optional modules. The target aggregator further takes care of the conflicting configurations and appropriately proceeds with the application of the cloning configuration.

## Topics:

- [clone-config apply](#)
- [clone-config check](#)
- [clone-config create](#)

## clone-config apply

Apply the cloning configuration file on the target aggregator.

**Syntax** `clone-config apply [file-name filename][output xml]`

<b>Parameters</b>	<b>apply</b>	Enter the keyword <code>apply</code> to apply the cloning configuration.
	<b>file-name</b> <b><i>filename</i></b>	Enter the keywords <code>file-name</code> to specify the user-defined cloning configuration file name in flash. By default, the file name is <code>cloning-config</code> .
	<b>output xml</b>	Enter the keywords <code>output xml</code> to enable the command output status to be displayed in the XML format.

**Defaults** `cloning-config`

**Command Modes** EXEC

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.10(0.0)</b>	Introduced on the FN IOM and M I/O Aggregator.

## clone-config check

Check the cloning configuration file compatibility with the current configurations on the target aggregator.

**Syntax** `clone-config check [file-name filename][output xml]`

<b>Parameters</b>	<b>check</b>	Enter the keyword <code>check</code> to check the cloning configuration compatibility.
	<b>file-name</b> <b><i>filename</i></b>	Enter the keywords <code>file-name</code> to specify the user-defined cloning configuration file name in flash. By default, the file name is <code>cloning-config</code> .
	<b>output xml</b>	Enter the keywords <code>output xml</code> to enable the command output status to be displayed in the XML format.

**Defaults** `cloning-config`

**Command Modes** EXEC

Command History	Version	Description
	9.10(0.0)	Introduced on the FN IOM and M I/O Aggregator.

## clone-config create

Create the cloning configuration.

**Syntax** `clone-config create [file-name filename][output xml]`

Parameters		
<b>create</b>		Enter the keyword <code>create</code> to create the cloning configuration file.
<b>file-name</b> <b><i>filename</i></b>		Enter the keywords <code>file-name</code> to save the cloning configuration in user-defined filename. By default, it gets stored in flash under the filename <code>cloning-config</code> .
<b>output xml</b>		Enter the keywords <code>output xml</code> to enable the command output status to be displayed in the XML format.

**Defaults** cloning-config

**Command Modes** EXEC

Command History	Version	Description
	9.10(0.0)	Introduced on the FN IOM and M I/O Aggregator.

# Content Addressable Memory (CAM)

Content addressable memory (CAM) commands are supported on the Dell Networking operating software on the platform.

**NOTE:** If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance.

## Topics:

- CAM Profile Commands

## 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).
- Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

## Important Points to Remember

- The Dell Networking Operating System (OS) versions supports CAM allocations.
- 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, 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-qos-
dual- number | vman-qos-dual-fp number] ipv4pbr number} ecfmac1 number
[nlbclusteraclnumber]fcoeacl number iscsioptacl number}
```

### Parameters

#### default

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

- L3 ACL (ipv4acl): 4
- L2 ACL(l2acl): 5
- IPv6 L3 ACL (ipv6acl): 0
- L3 QoS (ipv4qos): 1
- L2 QoS (l2qos): 1
- L2PT (L2PT): 0
- MAC ACL (IpMacAcl): 0
- VmanDualQos: 0

- EcfmAcl: 0
- nlbclusteracl: 0
- FcoeAcl: 4
- iscsiOptAcl: 2

<b>l2acl number</b>	Enter the keyword <code>l2acl</code> and then the number of l2acl blocks. The range is from 1 to 8.
<b>ipv4acl number</b>	Enter the keyword <code>ipv4acl</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.
<b>ipv6acl number</b>	Enter the keyword <code>ipv6acl</code> and then the number of FP blocks for IPv6. The range is from 0 to 4.
<b>ipv4qos number</b>	Enter the keyword <code>ipv4qos</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.
<b>l2qos number</b>	Enter the keyword <code>l2qos</code> and then the number of FP blocks for l2 qos. The range is from 1 to 8.
<b>l2pt number</b>	Enter the keyword <code>l2pt</code> and then the number of FP blocks for l2 protocol tunnelling. The range is from 0 to 1.
<b>ipmacacl number</b>	Enter the keyword <code>ipmacacl</code> and then the number of FP blocks for IP and MAC ACL. The range is from 0 to 6.
<b>ecfmacl number</b>	Enter the keyword <code>ecfmacacl</code> and then the number of FP blocks for ECFM ACL. The range is from 0 to 5.
<b>nlbclusteracl number</b>	Enter the keyword <code>nlbclusteracl</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 eight NLB arp entries reserved for internal functionality.
	<b>i NOTE:</b> When you reconfigure CAM allocation, use the <code>nlbclusteracl number</code> 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 upto 256 CAM entries. Select 1 to configure 128 entries. Select 2 to configure 256 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.
<b>vman-qos vman-dual-qos number</b>	Enter the keyword <code>vman-qos</code> and then the number of FP blocks for VMAN QoS. The range is from 0 to 6.
<b>vman-dual-qos number</b>	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.
<b>ipv4pbr number</b>	Enter the keyword <code>ipv4pbr</code> and then the number of FP blocks for ipv4pbr ACL. The range is from 0 to 8.
<b>Openflow number</b>	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.
<b>fcoeacl number</b>	Enter the keyword <code>fcoeacl</code> and then the number of FP blocks for FCOE ACL. The range is from 0 to 6.
<b>iscsioptacl number</b>	Enter the keyword <code>iscsioptacl</code> and then the number of FP blocks for iSCSI optimization ACL. The range is from 0 to 2.
<b>l2acl number</b>	Allocate space to each CAM region.
<b>ipv4acl number</b>	Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The range for <code>ipv4acl</code> is from 1 to 4. The <code>ipv6acl</code> range must be a factor of 2.
<b>ipv6acl number</b>	
<b>ipv4qos number</b>	
<b>l2qos number</b>	
<b>l2pt number</b>	
<b>ipmacacl number</b>	The total space allocated must equal 13.
<b>ecfmacl number</b>	The range for <code>ipv4acl</code> is 1 to 4.



**[vman-qos | vman--qos-dual number | vman-qos-dual-fp number] ipv4pbr number**

The `ipv6acl` range must be a factor of 2.

The `vman-qos-dual-fp number` must be entered as a multiple of 4.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Added the keyword <code>n1bcluster ACL</code> .
	<b>9.4.(0.0)</b>	Added support for PBR.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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. The `ipv4acl` profile range is from 1 to 4.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

On the switch, there can be only one odd number of Blocks in the CLI configuration; the other Blocks must be in factors of two. For example, a CLI configuration of 5+4+2+1+1 Blocks is not supported; a configuration of 6+4+2+1 Blocks is supported.

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 two (2, 4, 6, 8, 10).

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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).

**i 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-mapsections* in the *Dell Networking Operating System Configuration Guide*.

## cam-threshold

Configure CAM threshold value for sending the syslog message on CAM usage. Configure silence period for stop receiving syslog message on CAM usage.

**Syntax** `cam-threshold threshold {default | threshold-percent} silence-period {default | silence-period-value}`



### NOTE:

This command is applicable only in Full-Switch mode.

**Defaults** Enabled

### Parameters

<b>threshold default</b>	Enter the keyword <code>default</code> for CAM usage threshold for notification of the CAM usage through syslog message. The default threshold value is <b>90</b> percent.
<b>threshold <i>threshold-percent</i></b>	Enter the threshold percent for notification of the CAM usage through syslog message. The range is from 1 to 100 percent.
<b>silence-period default</b>	Enter the keyword <code>default</code> to set the silence period for receiving syslog message regarding CAM usage for CAM region, slot/portpipe. The default silence period is <b>0</b> seconds.
<b>silence-period <i>silence-period-value</i></b>	Enter the silence period for stop receiving syslog message for the respective CAM region, slot/portpipe. The range is from 0 to 65535 seconds.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.14.1.0</b>	Introduced on the S4810 and S4820T.
<b>9.13.0.0</b>	Introduced on the MXL, FN IOM, S5000, S4048-ON, S6000, S6000-ON, S3048-ON, S3100 Series, C9010, S4048T-ON, Z9500, Z9100-ON, S6100-ON, S6010-ON.

### Usage Information

The `no cam-threshold` command will set the CAM threshold to 90 percent and silence period to 0. The CAM threshold and silence period configuration is applicable only for Ingress L2, IPv4, IPv6 and Egress L2, IPv4, and IPv6 ACL CAM groups. For other ACL CAM regions, the CAM threshold and silence period is not configurable and the values are fixed to 90 percent and 0 respectively.

### Example

```
DellEMC(conf)#cam-threshold threshold 2 silence-period 2
DellEMC(conf)#do show running-config | g cam-threshold
cam-threshold threshold 2 silence-period 2
```

## show cam-acl

Display the details of the CAM profiles on the chassis and all stack units.

**Syntax** `show cam-acl`

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The display reflects the settings implemented with the `cam-acl` command.

**Example (Default)**

```
Dell#show cam-acl

-- Chassis Cam ACL --
      Current Settings(in block sizes)
      1 block = 128 entries
L2Acl      :      6
Ipv4Acl    :      4
Ipv6Acl    :      0
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  :      0
nlbclusteracl:      0

-- stack-unit 0 --
      Current Settings(in block sizes)
      1 block = 128 entries
L2Acl      :      6
Ipv4Acl    :      4
Ipv6Acl    :      0
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  :      0
nlbclusteracl:      0

-- stack-unit 1 --
      Current Settings(in block sizes)
      1 block = 128 entries
L2Acl      :      6
Ipv4Acl    :      4
Ipv6Acl    :      0
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      :      0
nlbclusteracl :      0
```

## show cam-acl-egress

Display the details of the FP groups allocated for the egress ACL.

**Syntax** `show cam-acl-egress`

**Defaults** none

**Command Modes** Configuration

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The display reflects the settings implemented with the `cam-acl-egress` command.

**Example**

```
Dell#show cam-acl-egress

-- Chassis Egress Cam ACL --
      Current Settings(in block sizes)
L2Acl   :      1
Ipv4Acl :      1
Ipv6Acl :      2

-- Stack unit 0 --
      Current Settings(in block sizes)
L2Acl   :      1
Ipv4Acl :      1
Ipv6Acl :      2

Dell#
```

# Control Plane Policing (CoPP)

The Dell Networking OS supports the following CoPP commands.

## Topics:

- [control-plane-cpuqos](#)
- [service-policy rate-limit-cpu-queues](#)
- [service-policy rate-limit-protocols](#)
- [show cpu-queue rate cp](#)
- [show ip protocol-queue-mapping](#)
- [show ipv6 protocol-queue-mapping](#)
- [show mac protocol-queue-mapping](#)

## control-plane-cpuqos

To manage control-plane traffic, enter control-plane mode and configure the switch.

**Syntax** `control-plane-cpuqos`

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## service-policy rate-limit-cpu-queues

Apply a policy map for the system to rate limit control traffic on a per-queue basis.

**Syntax** `service-policy rate-limit-cpu-queues policy-name`

**Parameters** *policy-name* Enter the service-policy name, using a string up to 32 characters.

**Defaults** Not configured.

**Command Modes** CONTROL-PLANE-CPUQOS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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, do not use the keywords `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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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, do not use the keywords `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 queue.

**Syntax** `show cpu-queue rate cp`

**Defaults** Not configured.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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#						

## 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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#
```

## 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

**Supported Modes** Full-Switch

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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      -
        09:00:2b:00:00:04/05  any      Q9      CP      -
Dell#
```



## u-Boot

All commands in this chapter are in u-Boot mode. These commands are supported on the Dell Networking Aggregator only.

To access this mode, hit any key when the following line appears on the console during a system boot: Hit any key to stop autoboot:

You enter u-Boot immediately, as indicated by the `BOOT_USER#` prompt.

**i** **NOTE:** Only the most frequently used commands available in uBoot mode are described in this chapter.

In uBoot mode, you cannot use the Tab key for command completion.

### Topics:

- [boot change](#)
- [boot show net config retries](#)
- [boot write net config retries](#)
- [boot zero](#)
- [default gateway](#)
- [enable](#)
- [help](#)
- [ignore enable password](#)
- [ignore startup-config](#)
- [interface management ethernet ip address](#)
- [no default gateway](#)
- [no interface management ethernet ip address](#)
- [reload](#)
- [show boot blc](#)
- [show boot selection](#)
- [show bootflash](#)
- [show bootvar](#)
- [show default gateway](#)
- [show interface management ethernet](#)
- [show interface management port config](#)
- [syntax help](#)

## boot change

Change the operating system boot parameters.

**Syntax** `boot change [primary | secondary | default]`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## boot show net config retries

Show the number of retries for network boot configuration failure.

**Syntax** `boot show net config retries`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER# boot show net config retries
Number of Network Boot Config Retries is : 0
BOOT_USER #
```

## boot write net config retries

Set the number of retries for network boot configuration failure.

**Syntax** `boot write net config retries <int>`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER # boot write net config retries 2
Updated number of Network Boot Config retries to 2.
BOOT_USER #
```

## boot zero

Clears the primary, secondary, or default boot parameters.

**Syntax** `boot zero [primary| secondary| default]`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# default gateway

Set the default gateway IP address.

**Syntax** default-gateway <ip-address>

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# enable

Change the access privilege level.

**Syntax** enable [user| admin]

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# help

Displays the help menu.

**Syntax** help

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
boot change [primary|secondary|default]
    change operating system boot parameters
boot selection [a|b]
    change the rom bootstrap bootflash partition
boot show net config retries
```

```

    show number of retries for network boot config failure
boot write net config retries <int>
    write number of retries for network boot config failure
boot zero [primary|secondary|default]
    zero operating system boot parameters
default-gateway <ip-address>
    default-gateway - set the default gateway ip address
enable [user|admin]
    change access privilege level
help
    display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #

```

## ignore enable password

Ignore the enabled password.

**Syntax** `ignore enable-password`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## ignore startup-config

Ignore the system startup configuration.

**Syntax** `ignore startup-config`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## interface management ethernet ip address

Set the management port IP address and mask.

**Syntax** `interface management ethernet ip address <ip/mask>`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

<b>Version</b>	<b>Description</b>
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## no default gateway

Clear the default gateway IP address.

**Syntax** `no default-gateway`

**Command Modes** uBoot

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## no interface management ethernet ip address

Clear the management port IP address and mask.

**Syntax** `no interface management ethernet ip address`

**Command Modes** uBoot

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## reload

Reload the switch.

**Syntax** `reload`

**Command Modes** uBoot

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# show boot blc

Show the boot loop counter value.

**Syntax** show boot blc

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER # show boot blc ?
Total 1 possible command found.
Possible command list:
show boot blc
    show the boot loop counter value
BOOT_USER # show boot blc
Boot Loop Counter : 10

BOOT_USER #
```

# show boot selection

Displays the ROM bootstrap bootflash partition.

**Syntax** show boot selection

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER # show boot blc ?
Total 1 possible command found.
Possible command list:
show boot blc
    show the boot loop counter value
BOOT_USER # show boot blc
Boot Loop Counter : 10

BOOT_USER #
```

# show bootflash

Show the summary of boot flash information.

**Syntax** show bootflash

**Command Modes** uBoot

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example**

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
=====
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Bootflash Partition B:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Boot Selector Partition:
  Dell Force10 Networks System Boot
  Official IOM_XLOAD_LP_IMG_BOOT_SELECTOR, BSP Release 4.0.0.0bt1
  Created Tue May 1 10:56:34 2012 by build on login-sjc-01

BOOT_USER #
```

## show bootvar

Show the summary of operating system boot parameters.

**Syntax** show bootvar

**Command Modes** uBoot

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example**

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
=====
boot device                : tftp
file name                   : premnath
Management Ethernet IP address : 10.16.130.134/16
Server IP address           : 10.16.127.35
Default Gateway IP address   : 15.0.0.1
Management Ethernet MAC address : 00:01:E8:43:DE:DF

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
=====
No Operating System boot parameters specified!

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
=====
boot device                : tftp
```

```
file name : FTOS-XL-8-3-16-99.bin
Management Ethernet IP address : 10.16.130.134/16
Server IP address : 10.16.127.53
Default Gateway IP address : 15.0.0.1
Management Ethernet MAC address : 00:01:E8:43:DE:DF

BOOT_USER #
```

## show default gateway

Displays the default gateway IP address.

**Syntax** `show default-gateway`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER # show default-gateway
Gateway IP address: 15.0.0.1
BOOT_USER #
```

## show interface management ethernet

Show the management port IP address and mask.

**Syntax** `show interface management ethernet`

**Command Modes** uBoot

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
BOOT_USER # show interface management ethernet
Management ethernet IP address: 10.16.130.134/16
BOOT_USER #
```

## show interface management port config

Show the management port boot characteristics.

**Syntax** `show interface management port config`

**Command Modes** uBoot

**Supported Modes** All Modes



**Command History****Version****Description****9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

**8.3.17.0**

Supported on the M I/O Aggregator.

**Example**

```
BOOT_USER # show interface management port config
Management ethernet Port Configuration: no Auto Negotiate
Management ethernet Port Configuration: 100M
Management ethernet Port Configuration: full duplex
BOOT_USER #
```

## syntax help

Show the syntax information.

**Syntax** help**Command Modes** uBoot**Supported Modes** All Modes**Command History****Version****Description****9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

**8.3.17.0**

Supported on the M I/O Aggregator.

# 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. DCB features are auto-configured in standalone mode.

The Dell Networking OS commands for DCB features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

CLI commands for individual DCB features are as follows:

## DCB command

- `dcb enable auto-detect on-next-reload`
- `show qos dcb-map`

## PFC Commands

- `clear pfc counters`
- `show interface pfc`
- `show interface pfc statistics`

## ETS Commands

- `clear ets counters`
- `show interface ets`

## DCBX Commands

- `dcbx version`
- `clear dcbx counters`
- `show dcb`
- `show interface dcbx detail`

## Topics:

- `advertise dcbx-appln-tlv`
- `advertise dcbx-tlv`
- `bandwidth-percentage`
- `dcb-enable`
- `dcb-policy buffer-threshold (Global Configuration)`
- `dcb-policy buffer-threshold (Interface Configuration)`
- `clear dcbx counters`
- `clear ets counters`
- `clear pfc counters`
- `dcb enable pfc-queues`
- `dcb enable auto-detect on-next-reload`
- `dcb-map stack-unit all stack-ports all`
- `dcbx-port role`
- `dcbx version`
- `debug dcbx`
- `description`
- `fc-map`
- `fcoe-map`
- `fcoe priority-bits`
- `iscsi priority-bits`
- `keepalive`
- `interface vlan (NPIV proxy gateway)`
- `pfc mode on`
- `pfc no-drop queues`

- [priority](#)
- [priority-group bandwidth pfc](#)
- [priority-pgid](#)
- [qos-policy-output ets](#)
- [qos-policy-buffer](#)
- [priority-list](#)
- [scheduler](#)
- [show dcb](#)
- [show interface dcbx detail](#)
- [show interface ets](#)
- [show interface pfc](#)
- [show interface pfc statistics](#)
- [show qos priority-groups](#)
- [show qos dcb-map](#)
- [show stack-unit stack-ports ets details](#)
- [dcb pfc-shared-buffer-size](#)
- [dcb pfc-total-buffer-size](#)
- [dcb-buffer-threshold](#)
- [dcb enable pfc-queues](#)
- [dcb {ets | pfc} enable](#)
- [service-class buffer shared-threshold-weight](#)
- [show stack-unit stack-ports pfc details](#)

## advertise dcbx-appln-tlv

On a DCBX port with a manual role, configure the application priority TLVs advertised on the interface to DCBX peers.

**Syntax** `advertise dcbx-appln-tlv {fcoe | iscsi}`

To remove the application priority TLVs, use the `no advertise dcbx-appln-tlv {fcoe | iscsi}` command.

**Parameters** `{fcoe | iscsi}` Enter the application priority TLVs, where:

- `fcoe`: enables the advertisement of FCoE in application priority TLVs.
- `iscsi`: enables the advertisement of iSCSI in application priority TLVs.

**Defaults** Application priority TLVs are enabled to advertise FCoE and iSCSI.

**Command Modes** PROTOCOL LLDP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-appln-tlv iscsi`.

# 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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	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.

# bandwidth-percentage

Assign a percentage of weight to the class/queue.

**Syntax** `bandwidth-percentage percentage`  
To remove the bandwidth percentage, use the `no bandwidth-percentage` command.

**Parameters** **percentage** Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).

**Defaults** none

**Command Modes** CONFIGURATION (conf-qos-policy-out)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

The unit of bandwidth percentage is 1%. A bandwidth percentage of 0 is allowed and disables the scheduling of that class. 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.

## dcb-enable

Enable data center bridging.

**Syntax** `dcb enable`  
To disable DCB, use the `no dcb enable` command.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.

#### Usage Information

DCB is not supported if you enable `link-level flow control` on one or more interfaces.

## dcb-policy buffer-threshold (Global Configuration)

Assign the dcb buffer threshold policy on the stack ports. To apply the dcb buffer threshold policy on the stack-units, use the configuration mode. To apply on front-end ports, use the interface mode.

**Syntax** `dcb-policy buffer-threshold stack-unit all stack-ports all profile-name`

#### Parameters

<b>dcb-buffer-threshold</b>	Configure the profile name for the DCB buffer threshold.
<b>profile-name</b>	Enter the name of the profile, which can be a string of up to 32 characters in length.
<b>stack-unit all</b>	Enter the stack unit identification. Indicates the specific the stack unit or units. Entering all shows the status for all stacks.
<b>stack-port all</b>	Enter the port number of a port in a switch stack.

**Default** None

**Command Modes** CONFIGURATION mode

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th>Version</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.3(0.0)</b></td> <td>Introduced on the MXL platform.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.3(0.0)</b>	Introduced on the MXL platform.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.3(0.0)</b>	Introduced on the MXL platform.						
<b>Usage Information</b>	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 for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to manage and administer the behavior of lossless queues.						
<b>Example for Configuration Mode</b>	<code>Dell(conf)# dcb-policy buffer-threshold stack-unit all stack-ports all test</code>						
<b>Example for Interface Mode</b>	<code>Dell(conf-if-te-1/1)#dcb-policy buffer-threshold test</code>						

## 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.

<b>Syntax</b>	<code>dcb-policy buffer-threshold <i>profile-name</i></code>						
<b>Parameters</b>	<table border="0"> <tr> <td><b>buffer-threshold</b></td> <td>Configure the profile name for the DCB buffer threshold</td> </tr> <tr> <td><b><i>profile-name</i></b></td> <td>Enter the name of the profile, which can be a string of up to 32 characters in length.</td> </tr> </table>	<b>buffer-threshold</b>	Configure the profile name for the DCB buffer threshold	<b><i>profile-name</i></b>	Enter the name of the profile, which can be a string of up to 32 characters in length.		
<b>buffer-threshold</b>	Configure the profile name for the DCB buffer threshold						
<b><i>profile-name</i></b>	Enter the name of the profile, which can be a string of up to 32 characters in length.						
<b>Default</b>	None						
<b>Command Modes</b>	INTERFACE mode						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table border="0"> <thead> <tr> <th>Version</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.3(0.0)</b></td> <td>Introduced on the MXL platform.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.3(0.0)</b>	Introduced on the MXL platform.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.3(0.0)</b>	Introduced on the MXL platform.						
<b>Usage Information</b>	You can configure 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.						
<b>Example</b>	<code>Dell(conf-if-te-0/0)#dcb-policy buffer-threshold test</code>						

## clear dcbx counters

Clear all DCBx TLV counters on an interface.

<b>Syntax</b>	<code>clear dcbx counters tengigabitethernet slot/port</code>
<b>Defaults</b>	none
<b>Command Modes</b>	EXEC Privilege
<b>Supported Modes</b>	All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## clear ets counters

Clear ETS TLV counters.

**Syntax** `clear ets counters [tengigabitethernet slot/port]`

**Parameters** **slot/port** Enter the slot/port number.

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## 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 [statistics]] | [stack-unit {unit-number | all} stack-ports all]`

**Parameters**

- port-type** Enter the keywords `port-type` then the slot/port information.
- stack-unit *unit number*** Enter the keywords `stack-unit` then the stack-unit number to clear. The range is from 0 to 5.
- all stack-ports all** Enter the keywords `all stack-ports all` to clear the counters on all interfaces.
- statistics** Enter the keyword `statistics` to clear only the hardware PFC counters.

**Defaults** None

**Command Modes** • EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage information** If you do not use the `statistics` parameter, both hardware and DCBx counters clear.

# dcb enable pfc-queues

Configure the number of PFC queues.

**Syntax** `dcb enable pfc-queues value`

**Parameters** **value** Enter the number of PFC queues. The range is from 1 to 4. The number of ports supported based on lossless queues configured will depend on the buffer.

**Default** 2

**Command Modes** CONFIGURATION mode

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the MXL 10/40GbE Switch IO Module platform.

**Usage Information** You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

**Example** `Dell(conf)#dcb pfc-queues 4`

# dcb enable auto-detect on-next-reload

Enables or disables global DCB on a subsequent reload. Also internally configures PFC buffers based on DCB enable or disable. You must save and reload for the configurations to take effect. You can use the `auto-detect` keyword to re-enable IOA with the port-wise DCB auto detect feature.

**Syntax** `dcb enable [auto-detect | on-next-reload]`  
To disable global DCB on a subsequent reload, use the `no dcb enable on-next-reload` command.

**Parameters** **auto-detect** Enter the keywords `auto-detect` to re-enable the Aggregator with port wise DCB auto detect feature.  
**on-next-reload** Enter the keywords `on-next-reload` to apply DCB configurations on subsequent reload.

**Defaults** DCB is globally enabled with auto-detect feature.

**Command Modes** • CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.3</b>	Added auto-detect parameter on the M I/O Aggregator.



## Version Description

8.3.17.0 Supported on the M I/O Aggregator.

### Example (Disable)

```
Dell#show dcb stack-unit 0 port-set 0
stack-unit 0 port-set 0
DCB Status: Enabled, PFC Queue Count: 4

stack-unit Total Buffer PFC Total Buffer PFC Shared Buffer PFC Available Buffer
PP (KB) (KB) (KB) (KB)
-----
0 0 3822 1912 832 450
Dell(conf)#
Dell#
Dell#
Dell#conf
Dell(conf)#no dcb enable on-next-reload
Dell(conf)#end
Dell#
Dell#write memory
!
Mar 18 00:21:49: %STKUNIT0-M:CP %FILEMGR-5-FILESAVED:
 Copied running-config to startup-config in flash by default

Dell#reload

Proceed with reload [confirm yes/no]: y
syncing disks... done
unmounting file systems...
unmounting /f10/flash (/dev/ld0e)...
unmounting /usr (mfs:35)...
unmounting /lib (mfs:24)...
unmounting /f10 (mfs:21)...
unmounting /tmp (mfs:15)...
unmounting /kern (kernfs)...
unmounting / (/dev/md0a)... done
rebooting...

Dell#show dcb stack-unit 0 port-set 0
stack-unit 0 port-set 0
DCB Status: Enabled, PFC Queue Count: 4

stack-unit Total Buffer PFC Total Buffer PFC Shared Buffer PFC Available Buffer
P (KB) (KB) (KB) (KB)
-----
0 0 3822 1912 832 450
Dell(conf)#
Dell#
```

### Example (Enable)

```
Dell#show dcb stack-unit 0 port-set 0
stack-unit 0 port-set 0
DCB Status: Enabled, PFC Queue Count: 4

stack-unit Total Buffer PFC Total Buffer PFC Shared Buffer PFC Available Buffer
PP (KB) (KB) (KB) (KB)
-----
0 0 3822 1912 832 450
Dell(conf)#
Dell#
Dell#
Dell#
Dell#conf
Dell(conf)#dcb enable on-next-reload
Dell(conf)#end
Dell#Mar 18 00:26:07: %STKUNIT0-M:CP %SYS-5-CONFIG_I:
 Configured from console

Dell#write memory
!
Mar 18 00:26:11: %STKUNIT0-M:CP %FILEMGR-5-FILESAVED:
 Copied running-config to startup-config in flash by default

Dell#
Dell#reload

Proceed with reload [confirm yes/no]: y
syncing disks... done
unmounting file systems...
unmounting /f10/flash (/dev/ld0e)...
unmounting /usr (mfs:35)...
unmounting /lib (mfs:24)...
unmounting /f10 (mfs:21)...
unmounting /tmp (mfs:15)...
unmounting /kern (kernfs)...
unmounting / (/dev/md0a)... done
rebooting...
Dell#show dcb stack-unit 0 port-set 0
stack-unit 0 port-set 0
DCB Status: Enabled, PFC Queue Count: 4

stack-unit Total Buffer PFC Total Buffer PFC Shared Buffer PFC Available Buffer
PP (KB) (KB) (KB) (KB)
-----
0 0 3822 1912 832 450
Dell(conf)#
```

### Example (Enable DCB with Auto-Detect)

```
Dell#show dcb
stack-unit 0 port-set 0
DCB Status : Disabled
PFC Queue Count : 2
Total Buffer[lossy + lossless] (in KB) : 3822
PFC Total Buffer (in KB) : 1912
PFC Shared Buffer (in KB) : 832
PFC Available Buffer (in KB) : 1080
Dell#
Dell#
Dell#con
Dell(conf)#dcb enable auto-detect on-next-reload
```

```

Dell(conf)#end
Dell#Mar 18 00:35:19: %STKUNIT0-M:CP %SYS-5-CONFIG_I
: Configured from console

Dell#write memory
!
Mar 18 00:35:24: %STKUNIT0-M:CP %FILEMGR-5-FILESAVED:
Copied running-config to startup-config in flash by default

Dell#
Dell#reload

Proceed with reload [confirm yes/no]: y
syncing disks... done
unmounting file systems...
unmounting /f10/flash (/dev/ld0e)...
unmounting /usr (mfs:35)...
unmounting /lib (mfs:24)...
unmounting /f10 (mfs:21)...
unmounting /tmp (mfs:15)...
unmounting /kern (kernfs)...
unmounting / (/dev/md0a)... done
rebooting...
Dell#show dcb stack-unit 0 port-set 0
stack-unit 0 port-set 0
DCB Status: Enabled, PFC Queue Count: 4

stack-unit  Total Buffer PFC  Total Buffer PFC  Shared Buffer PFC  Available Buffer
PP          (KB)          (KB)          (KB)          (KB)
-----
0           0           3822          1912          832          450
Dell(conf)#

```

## dcb-map stack-unit all stack-ports all

Apply the specified DCB map on all ports of the switch stack.

<b>Syntax</b>	<code>dcb-map stack-unit all stack-ports all <i>dcb-map-name</i></code>								
	To remove the PFC and ETS settings in a DCB map from all stack units, use the <code>no dcb-map stack-unit all stack-ports all</code> command.								
<b>Parameters</b>	<b><i>dcb-map-name</i></b> Enter the name of the DCB map.								
<b>Defaults</b>	None								
<b>Command Modes</b>	CONFIGURATION								
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch								
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> <tr> <td><b>9.3(0.0)</b></td> <td>Introduced on the FC Flex IO Modules with I/O Aggregator.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.3(0.0)</b>	Introduced on the FC Flex IO Modules with I/O Aggregator.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>9.3(0.0)</b>	Introduced on the FC Flex IO Modules with I/O Aggregator.								
<b>Usage Information</b>	The <code>dcb-map stack-unit all stack-ports all</code> command overwrites any previous DCB maps applied to stack ports.								

## dcbx-port role

Configure the DCBX port role the interface uses to exchange DCB information.

<b>Syntax</b>	<code>dcbx port-role {config-source   auto-downstream   auto-upstream   manual}</code>								
	To remove DCBX port role, use the <code>no dcbx port-role {config-source   auto-downstream   auto-upstream   manual}</code> command.								
<b>Parameters</b>	<table border="0"> <tr> <td><b>config-source  </b></td> <td>Enter the DCBX port role, where:</td> </tr> <tr> <td><b>auto-downstream  </b></td> <td>• <code>config-source</code>: configures the port to serve as the configuration source on</td> </tr> <tr> <td><b>auto-upstream  </b></td> <td>the switch.</td> </tr> <tr> <td><b>manual</b></td> <td></td> </tr> </table>	<b>config-source  </b>	Enter the DCBX port role, where:	<b>auto-downstream  </b>	• <code>config-source</code> : configures the port to serve as the configuration source on	<b>auto-upstream  </b>	the switch.	<b>manual</b>	
<b>config-source  </b>	Enter the DCBX port role, where:								
<b>auto-downstream  </b>	• <code>config-source</code> : configures the port to serve as the configuration source on								
<b>auto-upstream  </b>	the switch.								
<b>manual</b>									

- `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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

**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 `no 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 CEE (Intel 1.01).
- `cin`: configures the port to use Cisco-Intel-Nuova (DCBX 1.0).
- `ieee-v2.5`: configures the port to use IEEE 802.1az (Draft 2.5).

**Defaults** **Auto**

**Command Modes** INTERFACE PROTOCOL LLDP

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

**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.

# debug dcbx

Enable DCBX debugging.

**Syntax** `debug dcbx {all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}`

To disable DCBX debugging, use the `no debug dcbx` command.

**Parameters** `{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}`

Enter the type of debugging, where:

- `all`: enables all DCBX debugging operations.
- `auto-detect-timer`: enables traces for DCBX auto-detect timers.
- `config-exchng`: enables traces for DCBX configuration exchanges.
- `fail`: enables traces for DCBX failures.
- `mgmt`: enables traces for DCBX management frames.
- `resource`: enables traces for DCBX system resource frames.
- `sem`: enables traces for the DCBX state machine.
- `tlv`: enables traces for DCBX TLVs.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

## description

Enter a text description of the DCB policy (PFC input or ETS output).

**Syntax** `description text`

To remove the text description, use the `no description` command.

**Parameters** `text` Enter the description of the output policy. The maximum is 32 characters.

**Defaults** none

**Command Modes**

- DCB INPUT POLICY
- DCB OUTPUT POLICY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# fc-map

In an FCoE map, configure the FCoE mapped address prefix (FC-MAP) value which is used to identify FCoE traffic transmitted on the FCoE VLAN for the specified fabric.

**Syntax** `fc-map fc-map-value`

**Parameters** **fc-map-value** Enter the unique MAC address prefix used by a SAN fabric.  
The range of FC-MAP values is from 0EFC00 to 0EFCFF.

**Defaults** None

**Command Modes** FCoE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

The FC-MAP value you enter must match the FC-MAP value used by an FC switch or FCoE forwarder (FCF) in the fabric. An FCF switch accepts only FCoE traffic that uses the correct FC-MAP value.

The FC-MAP value is used to generate the fabric-provided MAC address (FP-MAC). The FPMA is used by servers to transmit FCoE traffic to the fabric. An FC-MAP can be associated with only one FCoE VLAN and vice versa.

In an FCoE map, the FC-MAP value, fabric ID, and FCoE VLAN parameters must be unique.

To remove a configured FC-MAP value from an FCoE map, enter the `no fc-map` command.

**Related Commands** [fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

# fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

**Syntax** `fcoe-map map-name`

**Parameters** **map-name** Maximum: 32 alphanumeric characters.

**Defaults** On the FN2210S Aggregator with PMUX modules, the following parameters are applied on all the PMUX module interfaces:

- Description: SAN\_FABRIC
- Fabric-id: 1002
- Fcoe-vlan: 1002
- Fc-map: 0x0efc00
- Fcf-priority: 128
- Fka-adv-period: 8000mSec
- Keepalive: enable

- Vlan priority: 3

**Command Modes** CONFIGURATION  
INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information** An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an FN2210S Aggregator with the PMUX module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric.

On an FN2210S Aggregator a with the PMUX module NPIV proxy gateway, you cannot apply an FCoE map applied on fabric-facing FC ports and server-facing 10-Gigabit Ethernet ports.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN used for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority used by a server, and the FIP keepalive (FKA) advertisement timeout.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique. Use one FCoE map to access one SAN fabric. You cannot use the same FCoE map to access different fabrics.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map map-name` command in Interface configuration mode.

## 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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

**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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

**Usage Information** This command is available at the global level only.

# keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

**Syntax** `keepalive [seconds]`  
To stop sending keepalive packets, use the `no keepalive` command.

**Parameters** `seconds` (OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is **10 seconds**.

**Defaults** Enabled.

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Introduced on the M I/O Aggregator.

**Usage Information** When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

# interface vlan (NPIV proxy gateway)

Create a dedicated VLAN to be used to send and receive Fibre Channel traffic over FCoE links between servers and a fabric over an Aggregator with the PMUX module of NPIV proxy gateway.

**Syntax** `interface vlan vlan-id`

**Parameters** `vlan-id` Enter a number as the VLAN Identifier. The range is 1 to 4094.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information**

FCoE storage traffic received from servers on an M I/O Aggregator with the PMUX module NPIV proxy gateway is de-capsulated into Fibre Channel packets and forwarded over FC links to SAN switches in a specified fabric. You must configure a separate FCoE VLAN for each fabric to which FCoE traffic is forwarded. Any non-FCoE traffic sent on a dedicated FCoE VLAN will be dropped.

You configure the association between a dedicated VLAN, which carries FCoE traffic from server CNAs over the NPIV proxy gateway to a SAN fabric in which destination storage arrays are installed, in an FCoE map by using the `fabric id vlan` command.

When you apply an FCoE map to a server-facing Ethernet port, the port is automatically configured as a tagged member of the FCoE VLAN.

For more information about VLANs and the commands to configure them, refer to the [Virtual LAN \(VLAN\) Commands](#) section.

## Example (Single Range)

```
Dell(conf)#interface vlan 10
Dell(conf-if-vl-3)#
```

# pfc mode on

Enable the PFC configuration on the port so that the priorities are included in DCBX negotiation with peer PFC devices.

**Syntax** `pfc mode on`  
To disable the PFC configuration, use the `no pfc mode on` command.

**Defaults** PFC mode is on.

**Command Modes** DCB MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.



## Usage Information

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

To disable PFC operation on an interface, enter the `no pfc mode on` command in DCB Input Policy Configuration mode. PFC is enabled and disabled as global DCB operation is enabled (`dcb-enable`) or disabled (`no dcb-enable`).

You cannot enable PFC and link-level flow control at the same time on an interface.

## 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 2-3`. The range is from 0 to 3.

### Defaults

No lossless queues are configured.

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

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

# priority

Configure the priority for the PFC threshold to be allocated to the buffer space parameters.

**Syntax** `priority value buffer-size size pause-threshold threshold-value resume-offset threshold-value shared-threshold-weight size`

<b>Parameters</b>	<b>priority</b>	Specify the priority of the queue for which the buffer space settings apply
	<b>value</b>	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
	<b>buffer-size</b>	Ingress buffer size
	<b>size</b>	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
	<b>pause-threshold</b>	Buffer limit for pause frames to be sent
	<b>threshold-value</b>	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.
	<b>resume-offset</b>	Buffer offset limit for resuming in KB
	<b>threshold-value</b>	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.
	<b>shared-threshold-weight</b>	Buffer shared threshold weight
	<b>size</b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**Usage Information** For each priority, you can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. When PFC detects congestion on a queue for a specified priority, it sends a pause frame for the 802.1p priority traffic to the transmitting device.

You can use the `priority` command to set up both the administrative and peer-related PFC priorities. For example, you can configure the intended buffer configuration for all 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-dcb-buffer-thr)#priority 0 buffer-size 52 pause-threshold 16 resume-offset 10 shared-threshold-weight 7
```

# priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

<b>Syntax</b>	<code>priority-group group-num {bandwidth percentage  strict-priority} pfc {on   off}</code>	
<b>Parameters</b>	<b>priority-group group-num</b>	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.
	<b>bandwidth percentage</b>	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%.
	<b>strict-priority</b>	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.
	<b>pfc {on   off}</b>	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.
<b>Defaults</b>	None	
<b>Command Modes</b>	DCB MAP	
<b>Supported Modes</b>	Programmable-Mux (PMUX)	
	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.
<b>Usage Information</b>	Use the <code>dcb-map</code> command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.	
	Use the <code>priority-pgid</code> 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 <code>priority-group bandwidth pfc</code> 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 <code>no priority-group bandwidth pfc</code> command.	
	By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the <code>bandwidth</code> 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.	
<b>Related Commands</b>	<a href="#">priority-pgid</a> – Configures the 802.1p priority traffic in a priority group for a DCB map.	

# priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

**Syntax** `priority-pgid dot1p0_group-num dot1p1_group-num dot1p2_group-num dot1p3_group-num dot1p4_group-num dot1p5_group-num dot1p6_group-num dot1p7_group-num`

**Parameters**

- `dot1p0_group-num`** Enter the priority group number for each 802.1p class of traffic in a DCB map.
- `dot1p1_group-num`**
- `dot1p2_group-num`**
- `dot1p3_group-num`**
- `dot1p4_group-num`**
- `dot1p5_group-num`**
- `dot1p6_group-num`**
- `dot1p7_group-num`**

**Defaults** None

**Command Modes** DCB MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Introduced on the FC Flex IO module installed in the M I/O Aggregator.

**Usage Information** PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.
- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a `priority-pgid` configuration from a DCB map, enter the `no priority-pgid` command.

**Related Commands** [priority-group bandwidth pfc](#)— Configures the ETS bandwidth allocation and the PFC setting used to manage the port traffic in an 802.1p priority group.

# qos-policy-output ets

To configure the ETS bandwidth allocation and scheduling for priority traffic, create a QoS output policy.

**Syntax** `qos-policy-output policy-name ets`  
To remove the QoS output policy, use the `no qos-policy-output ets` command.

**Parameters** **policy-name** Enter the policy name. The maximum is 32 characters.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**  
If an error occurs in an ETS output-policy configuration, the configuration is ignored and the scheduler and bandwidth allocation settings are reset to the ETS default values (all priorities are in the same ETS priority group and bandwidth is allocated equally to each priority).  
If an error occurs when a port receives a peer's ETS configuration, the port's configuration is reset to the previously configured ETS output policy. If no ETS output policy was previously applied, the port is reset to the default ETS parameters.

**Related Commands**

- [scheduler](#) — schedules the priority traffic in port queues.
- [bandwidth-percentage](#) — bandwidth percentage allocated to the priority traffic in port queues.

# 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.

**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`

<b>Parameters</b>	<b>policy-name</b>	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.
	<b>queue 0 to queue 7</b>	Specify the queue number to which the QoS policy buffer parameters apply
	<b>pause</b>	Pause frames to be sent at the specified buffer limit levels and pause packet settings
	<b>no-drop</b>	The packets for this queue must not be dropped
	<b>value</b>	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
	<b>buffer-size</b>	Ingress buffer size

<b>size</b>	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
<b>pause-threshold</b>	Buffer limit for pause frames to be sent
<b>threshold-value</b>	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.
<b>resume-offset</b>	Buffer offset limit for resuming in KB
<b>threshold-value</b>	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.
<b>shared-threshold-weight</b>	Buffer shared threshold weight
<b>size</b>	Weightage of the priorities on the shared buffer size in the system. Enter a number in the range from 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**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
```

## priority-list

Configure the 802.1p priorities for the traffic on which you want to apply an ETS output policy.

**Syntax** `priority-list value`

To remove the priority list, use the `no priority-list` command.


**Parameters** **value** Enter the priority list value. Separate priority values with a comma; specify a priority range with a dash; for example, `priority-list 3,5-7`. The range is from 0 to 7.

**Defaults** none  
**Command Modes** PRIORITY-GROUP  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** By default:

- All 802.1p priorities are grouped in priority group 0.
- 100% of the port bandwidth is assigned to priority group 0. The complete bandwidth is equally assigned to each priority class so that each class has 12 to 13%.

 **NOTE:** Please note that Dell Networking does not recommend to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

## scheduler

Configure the method used to schedule priority traffic in port queues.

**Syntax** `scheduler value`  
To remove the configured priority schedule, use the `no scheduler` command.

**Parameters** *value* Enter schedule priority value. The valid values are:

- `strict`: strict-priority traffic is serviced before any other queued traffic.
- `werr`: weighted elastic round robin (werr) provides low-latency scheduling for priority traffic on port queues.

**Defaults** Weighted elastic round robin (WERR) scheduling is used to queue priority traffic.

**Command Modes** POLICY-MAP-OUT-ETS

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** dot1p priority traffic on the switch is scheduled to the current queue mapping. dot1p priorities within the same queue must have the same traffic properties and scheduling method.

ETS-assigned scheduling applies only to data queues, not to control queues.

The configuration of bandwidth allocation and strict-queue scheduling is not supported at the same time for a priority group. If you configure both, the configured bandwidth allocation is ignored for priority-group traffic when you apply the output policy on an interface.

**Related Commands**

- [bandwidth-percentage](#) — bandwidth percentage allocated to priority traffic in port queues.

# 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]`

**Parameters** *unit number* Enter the DCB unit number. The range is from 0 to 5.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	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 0 port-set 0
DCB Status : Enabled
PFC Queue Count : 2
Total Buffer[lossy + lossless] (in KB) : 3822
PFC Total Buffer (in KB) : 1912
PFC Shared Buffer (in KB) : 832
PFC Available Buffer (in KB) : 1080
```

# show interface dcbx detail

Displays the DCBX configuration on an interface.

**Syntax** `show interface port-type slot/port dcbx detail`

**Parameters** *port-type* Enter the port type.  
*slot/port* Enter the slot/port number.

- NOTE:** This command also enables you to view information corresponding to a range of ports.
- You can specify multiple ports as *slot/port-range*. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	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
<b>Interface</b>	Interface type with chassis slot and port number.
<b>Port-Role</b>	Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.
<b>DCBX Operational Status</b>	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.
<b>Configuration Source</b>	Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).
<b>Local DCBX Compatibility mode</b>	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.
<b>Local DCBX Configured mode</b>	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).
<b>Peer Operating version</b>	DCBX version that the peer uses to exchange DCB parameters.
<b>Local DCBX TLVs Transmitted</b>	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
<b>Local DCBX Status: DCBX Operational Version</b>	DCBX version advertised in Control TLVs.
<b>Local DCBX Status: DCBX Max Version Supported</b>	Highest DCBX version supported in Control TLVs.
<b>Local DCBX Status: Sequence Number</b>	Sequence number transmitted in Control TLVs.
<b>Local DCBX Status: Acknowledgment Number</b>	Acknowledgement number transmitted in Control TLVs.
<b>Local DCBX Status: Protocol State</b>	Current operational state of the DCBX protocol: ACK or IN-SYNC.
<b>Peer DCBX Status: DCBX Operational Version</b>	DCBX version advertised in Control TLVs received from the peer device.
<b>Peer DCBX Status: DCBX Max Version Supported</b>	Highest DCBX version supported in Control TLVs received from the peer device.
<b>Peer DCBX Status: Sequence Number</b>	Sequence number transmitted in Control TLVs received from the peer device.

Field	Description
<b>Peer DCBX Status: Acknowledgment Number</b>	Acknowledgement number transmitted in Control TLVs received from the peer device.
<b>Total DCBX Frames transmitted</b>	Number of DCBX frames sent from the local port.
<b>Total DCBX Frames received</b>	Number of DCBX frames received from the remote peer port.
<b>Total DCBX Frame errors</b>	Number of DCBX frames with errors received.
<b>Total DCBX Frames unrecognized</b>	Number of unrecognizable DCBX frames received.

### Example

```

Dell(conf)# show interface tengigabitethernet 0/49 dcbx detail
Dell#show interface te 0/49 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 0/49
  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

```

# 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 ets {summary | detail}`

**Parameters**

<b><i>port-type slot/port ets</i></b>	Enter the port-type slot and port ETS information.
<b>{summary   detail}</b>	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.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To clear ETS TLV counters, use the `clear ets counters interface port-type slot/port` command.

The following describes the `show interface summary` command shown in the following example.

Field	Description
<b>Interface</b>	Interface type with stack-unit and port number.
<b>Max Supported TC Group</b>	Maximum number of priority groups supported.
<b>Number of Traffic Classes</b>	Number of 802.1p priorities currently configured.
<b>Admin mode</b>	ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.
<b>Admin Parameters</b>	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
<b>Remote Parameters</b>	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.
<b>Local Parameters</b>	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
<b>Operational status (local port)</b>	Port state for current operational ETS configuration: <ul style="list-style-type: none"><li><b>Init:</b> Local ETS configuration parameters were exchanged with the peer.</li><li><b>Recommend:</b> Remote ETS configuration parameters were received from the peer.</li></ul>

Field	Description
	<ul style="list-style-type: none"> <li>Internally propagated: ETS configuration parameters were received from the configuration source.</li> </ul>
<b>ETS DCBX Oper status</b>	Operational status of the ETS configuration on the local port: match or mismatch.
<b>Reason</b>	Reason displayed when the DCBX operational status for ETS on a port is down.
<b>State Machine Type</b>	Type of state machine used for DCBX exchanges of ETS parameters: Feature — for legacy DCBX versions; Asymmetric — for an IEEE version.
<b>Conf TLV Tx Status</b>	Status of ETS Configuration TLV advertisements: enabled or disabled.
<b>ETS TLV Statistic: Input Conf TLV pkts</b>	Number of ETS Configuration TLVs received.
<b>ETS TLV Statistic: Output Conf TLV pkts</b>	Number of ETS Configuration TLVs transmitted.
<b>ETS TLV Statistic: Error Conf TLV pkts</b>	Number of ETS Error Configuration TLVs received.

### Example (Summary)

```

Dell(conf)# show interfaces te 0/1 ets summary
Interface TenGigabitEthernet 0/1
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

```

### Example (Detail)

```

Dell(conf)# show interfaces tengigabitethernet 0/1 ets detail
Interface TenGigabitEthernet 0/1
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
ETS DCBX Oper status is Down
Reason: Port Shutdown
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

```

```
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
```

## 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 pfc {summary | detail}`

**Parameters**

<b><i>port-type slot/ port pfc</i></b>	Enter the port-type slot and port PFC information.
<b>{summary   detail}</b>	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.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes** INTERFACE

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To clear the PFC TLV counters, use the `clear pfc counters interface port-type slot/port` command.

The following describes the `show interface pfc summary` command shown in the following example.

Field	Description
<b>Interface</b>	Interface type with stack-unit and port number.
<b>Admin mode is on Admin is enabled</b>	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.
<b>Remote is enabled, Priority list Remote Willing Status is enabled</b>	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 disabled.
<b>Local is enabled</b>	DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.
<b>Operational status (local port)</b>	Port state for current operational PFC configuration: <ul style="list-style-type: none"> <li><code>Init</code>: Local PFC configuration parameters were exchanged with the peer.</li> <li><code>Recommend</code>: Remote PFC configuration parameters were received from the peer.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>Internally propagated: PFC configuration parameters were received from the configuration source.</li> </ul>
<b>PFC DCBX Oper status</b>	Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).
<b>Reason</b>	Reason displayed when the DCBx operational status for PFC on a port is down.
<b>State Machine Type</b>	Type of state machine used for DCBX exchanges of the PFC parameters: Feature — for legacy DCBX versions; Symmetric — for an IEEE version.
<b>TLV Tx Status</b>	Status of the PFC TLV advertisements: enabled or disabled.
<b>PFC Link Delay</b>	Link delay (in quanta) used to pause specified priority traffic.
<b>Application Priority TLV: FCOE TLV Tx Status</b>	Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
<b>Application Priority TLV: SCSI TLV Tx Status</b>	Status of iSCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
<b>Application Priority TLV: Local FCOE Priority Map</b>	Priority bitmap the local DCBX port uses in FCoE advertisements in application priority TLVs.
<b>Application Priority TLV: Local iSCSI Priority Map</b>	Priority bitmap the local DCBX port uses in iSCSI advertisements in application priority TLVs.
<b>Application Priority TLV: Remote FCOE Priority Map</b>	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
<b>Application Priority TLV: Remote iSCSI Priority Map</b>	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
<b>PFC TLV Statistics: Input TLV pkts</b>	Number of PFC TLVs received.
<b>PFC TLV Statistics: Output TLV pkts</b>	Number of PFC TLVs transmitted.
<b>PFC TLV Statistics: Error pkts</b>	Number of PFC error packets received.
<b>PFC TLV Statistics: Pause Tx pkts</b>	Number of PFC pause frames transmitted.
<b>PFC TLV Statistics: Pause Rx pkts</b>	Number of PFC pause frames received.

**Example (Summary)**

```
Dell# show interfaces tengigabitethernet 0/4 pfc summary
Interface TenGigabitEthernet 0/4
  Admin mode is on
```

```

Admin is enabled
Remote is enabled, Priority list is 4
Remote Willing Status is enabled
Local is enabled
Oper status is Recommended
PFC DCBX Oper status is Up
State Machine Type is Feature
TLV Tx Status is enabled
PFC Link Delay 45556 pause quantams
Application Priority TLV Parameters :
-----
FCOE TLV Tx Status is disabled
ISCSI TLV Tx Status is disabled
Local FCOE PriorityMap is 0x8
Local ISCSI PriorityMap is 0x10
Remote FCOE PriorityMap is 0x8
Remote ISCSI PriorityMap is 0x8

Dell# show interfaces tengigabitethernet 0/4 pfc detail
Interface TenGigabitEthernet 0/4
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 pfc statistics`

**Parameters**

- port-type*** Enter the port type.
- slot/port*** Enter the slot/port number.

**i** **NOTE:** This command also enables you to view information corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes** INTERFACE

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.



Version	Description
9.4(0.0)	Supported on the FN I/O aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Example (Summary)

```
Dell#show interfaces te 0/3 pfc statistics
Interface TenGigabitEthernet 0/3

Priority Rx XOFF Frames Rx Total Frames Tx Total Frames
-----
0          0          0          0
1          0          0          0
2          0          0          0
3          0          0          0
4          0          0          0
5          0          0          0
6          0          0          0
7          0          0          0
```

## show qos priority-groups

Displays the ETS priority groups configured on the switch, including the 802.1p priority classes and ID of each group.

**Syntax** `show qos priority-groups`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

**NOTE:** Please note that Dell Networking does not recommend to use this command as it has been deprecated in the current 9.4(0.0) release. A warning message appears when you try to run this command indicating that you have to use the `dcb-map` commands in the future.

### Example

```
Dell#show qos priority-groups
priority-group ipc
priority-list 4
set-pgid 2
```

## show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

**Syntax** `show qos dcb-map map-name`

**Parameters** *map-name* Displays the PFC and ETS parameters configured in the specified map.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information** Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports.

The following table describes the `show qos dcb-map` output shown in the example below.

<b>Field</b>	<b>Description</b>
<b>State</b>	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
<b>PFC Mode</b>	PFC configuration in DCB map: On (enabled) or Off.
<b>PG</b>	Priority group configured in the DCB map.
<b>TSA</b>	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
<b>BW</b>	Percentage of bandwidth allocated to the priority group.
<b>PFC</b>	PFC setting for the priority group: On (enabled) or Off.
<b>Priorities</b>	802.1p priorities configured in the priority group.

#### Example

```
Dell# show qos dcb-map dcbmap2

State      :Complete
PfcMode:ON
-----
PG:0 TSA:ETS BW:50 PFC:OFF
Priorities:0 1 2 4 5 6 7

PG:1 TSA:ETS BW:50 PFC:ON
Priorities:3
```

## show stack-unit stack-ports ets details

Displays the ETS configuration applied to egress traffic on stacked ports, including ETS Operational mode on each unit and the configured priority groups with dot1p priorities, bandwidth allocation, and scheduler type.

**Syntax** `show stack-unit {all | stack-unit} stack-ports {all | port-number} ets details`

**Parameters**

<b><i>stack-unit</i></b>	Enter the stack unit identification.
<b><i>port-number</i></b>	Enter the port number.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

Version	Description
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf)# show stack-unit all stack-ports all ets details

Stack unit 0 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
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
2
3
4
5
6
7
8

Stack unit 1 stack port all
Max Supported TC Groups is 4
Number of Traffic Classes is 1
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
2
3
4
5
6
7
8
```

## dcb pfc-shared-buffer-size

Configure the maximum amount of shared buffer size for PFC packets in kilobytes.

<b>Syntax</b>	<code>dcb pfc-shared-buffer-size <i>KB</i></code>	
<b>Parameters</b>	<b><i>KB</i></b>	Enter a number in the range of 0 to 7787.
<b>Default</b>	None.	
<b>Command Modes</b>	CONFIGURATION mode	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	9.3(0.0)	Introduced on the MXL platform.

## Usage Information

Configure the maximum shared buffer available for PFC traffic. You can choose to increase or decrease the shared buffer that is allocated in the system by default. Configure the shared buffer size 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 shared buffer size is more than the total PFC buffer size value, the configuration is not saved and a system logging message is generated as follows:

Shared-pfc-buffer-size <= (Total-pfc-buffer-size — Σpfc priority <> buffer-size on each port, priority).

```
Dell(conf)#dcb pfc-shared-buffer-size 2000
```

```
%ERROR: pfc shared buffer size configured cannot accommodate existing
buffer requirement in the system.
```

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.

## Example

```
Dell(conf)#dcb pfc-shared-buffer-size 5000
```

# dcb pfc-total-buffer-size

Configure the total buffer size for PFC in kilobytes.

**Syntax** `dcb pfc-total-buffer-size KB`

**Parameters** **KB** Enter a number in the range of 0 to 7787.

**Default** The default is 6592KB.

**Command Modes** CONFIGURATION mode

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.9(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

Configure the maximum buffer available for PFC traffic. You can choose to increase or decrease the buffer size that is allocated in the system by default. However, if you modify the PFC buffer size lower than the previously configured size, the system determines whether this reduction in size is valid without disrupting the existing configuration. In such a scenario, disable and re-enable DCB. For example, if you modify the total buffer size as 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 in process.

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.

d.

## 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.
```

# dcb-buffer-threshold

Configure the profile name for the DCB buffer threshold.

**Syntax** `dcb buffer-threshold profile-name`

**Parameters** ***profile-name*** Enter the name of the profile, which can be a string of up to 32 characters in length.

**Default** None

**Command Modes** CONFIGURATION mode

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**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** `Dell(conf)#dcb buffer-threshold test`

**Example of commands in dcb buffer-threshold mode**

```
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
```

```
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
```

```
priority value buffer-size size pause-threshold threshold-value resume-
offset threshold-value shared-threshold-weight size
```

```
Dell(conf-dcb-buffer-thr)#priority 0 buffer-size 52 pause-threshold 16
resume-offset 10 shared-threshold-weight 7
```

# dcb enable pfc-queues

Configure the number of PFC queues.

**Syntax** `dcb enable pfc-queues value`

**Parameters** ***value*** Enter the number of PFC queues. The range is from 1 to 4. The number of ports supported based on lossless queues configured will depend on the buffer.

**Command Modes** CONFIGURATION mode

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL platform.

**Usage Information** You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your

network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

**Example** `Dell(conf)#dcb pfc-queues 4`

## dcb {ets | pfc} enable

Enable priority flow control or enhanced transmission selection on interface.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3 (0.1)</b>	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.

## 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.

**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**

<b>buffer</b>	Define the shared buffer settings.
<b>shared-threshold-weight</b>	Specify the weight of a queue for the shared buffer space.
<b>queue 0 to queue 7</b>	To apply the shared-threshold weight, specify the queue number .
<b>number</b>	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

**Supported Modes** Full-Switch

**Usage Information** You can configure all the data queues. You can configure queues 0-7. The following table describes the mapping between the threshold weight of the shared buffer on the queue. It also shows the percentage of the available shared buffer used by the queues for each of the corresponding threshold weights of the shared buffer:

shared-threshold-weight on the queue	% of available shared buffer that can be consumed by the queue.
0	No dynamic sharing; shared buffer = 0.
1	0.77%
2	1.54%
3	3.03%
4	5.88%
5	11.11%
6	20%
7	33.33%
8	50%
9	66.67%
10	80%
11	88.89%

Command History	Version	Description
	9.9(0.0)	Introduced on the MXL.

**Example**

```
Dell(conf-if-te-1/8)#Service-class buffer shared-threshold-weight queue5
4 queue7 6
```

## show stack-unit stack-ports pfc details

Displays the PFC configuration applied to ingress traffic on stacked ports, including PFC Operational mode on each unit with the configured priorities, link delay, and number of pause packets sent and received.

**Syntax** `show stack-unit {all | stack-unit} stack-ports {all | port-number} pfc details`

**Parameters**

- stack-unit*** Enter the stack unit.
- port-number*** Enter the port number.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf)# show stack-unit all stack-ports all pfc details

stack unit 0 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts

stack unit 1 stack-port all
  Admin mode is On
  Admin is enabled, Priority list is 4-5
  Local is enabled, Priority list is 4-5
  Link Delay 45556 pause quantum
  0 Pause Tx pkts, 0 Pause Rx pkts
```



# Dynamic Host Configuration Protocol

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 configuration policies determined by network administrators.

An Aggregator can operate as a DHCP client. As a DHCP client, the Aggregator requests an IP address from a DHCP server.

The following types of DHCP commands are described in this chapter:

- DHCP Client Commands
- Other Commands supported by DHCP Client

## DHCP Client Commands

- `clear ip dhcp client statistics`
- `ip address dhcp`
- `release dhcp interface`
- `renew dhcp interface`
- `show ip dhcp client statistics`
- `show ip dhcp lease`

## Other Commands supported by DHCP Client

- `debug ip dhcp client events`
- `debug ip dhcp client packets`

## Topics:

- Commands to Configure the System to be a DHCP Server
- Commands to Configure the System to be a DHCP Client
- Other Commands Supported by the DHCP Client
- 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.

<b>Syntax</b>	<code>clear ip dhcp [binding {address}   conflict   server statistics]</code>	
<b>Parameters</b>	<b>binding</b>	Enter the keyword <code>binding</code> to delete all entries in the binding table.
	<b>address</b>	Enter the IP address to clear the binding entry for a single IP address.
	<b>conflicts</b>	Enter the keyword <code>conflicts</code> to delete all of the log entries created for IP address conflicts.
	<b>server statistics</b>	Enter the keywords <code>server statistics</code> to clear all the server counter information.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Entering <CR> after the <code>clear ip dhcp binding</code> command clears all the IPs from the binding table.	

## debug ip dhcp server

Display the Dell Networking OS debugging messages for DHCP.

<b>Syntax</b>	<code>debug ip dhcp server [events   packets]</code>	
<b>Parameters</b>	<b>events</b>	Enter the keyword <code>events</code> to display the DHCP state changes.
	<b>packet</b>	Enter the keyword <code>packet</code> to display packet transmission/reception.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ipv6 dhcp

To enable debug logs for DHCPv6 relay agent transactions.

<b>Syntax</b>	<code>debug ipv6 dhcp</code>	
	To disable the debug logs for DHCPv6 relay agent transactions, use the <code>debug ipv6 dhcp</code> command.	
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## default-router

Assign a default gateway to clients based on the address pool.

<b>Syntax</b>	<code>default-router address [address2...address8]</code>	
<b>Parameters</b>	<b>address</b>	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.
<b>Defaults</b>	none	
<b>Command Modes</b>	DHCP <POOL>	

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## disable

Disable the DHCP server.

**Syntax** `disable`  
DHCP Server is disabled by default. To enable the system to be a DHCP server, use the `no disable` command.

**Defaults** Disabled

**Command Modes** DHCP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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>

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## domain-name

Assign a domain to clients based on the address pool.

**Syntax** `domain-name name`

**Parameters** *name* Give a name to the group of addresses in a pool.

**Defaults** none

**Command Modes** DHCP <POOL>

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

<b>Syntax</b>	<code>excluded-address [address   low-address high-address]</code>	
<b>Parameters</b>	<b><i>address</i></b>	Enter a single address to be excluded from the pool.
	<b><i>low-address</i></b>	Enter the lowest address in a range of addresses to be excluded from the pool.
	<b><i>high-address</i></b>	Enter the highest address in a range of addresses to be excluded from the pool.
<b>Defaults</b>	none	
<b>Command Modes</b>	DHCP	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## hardware-address

For manual configurations, specify the client hardware address.

<b>Syntax</b>	<code>hardware-address address</code>	
<b>Parameters</b>	<b><i>address</i></b>	Enter the hardware address of the client.
<b>Defaults</b>	none	
<b>Command Modes</b>	DHCP <POOL>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## host-address

For manual (rather than automatic) configurations, assign a host to a single-address pool.

<b>Syntax</b>	<code>host-address address</code>	
<b>Parameters</b>	<b><i>address</i></b>	Enter the host IP address.
<b>Defaults</b>	None	
<b>Command Modes</b>	DHCP-POOL	

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

Version	Description
9.14.1.3	This command replaces <code>host</code> command. Introduced on S3048-ON, S4048-ON, S4048T-ON, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, S3100, S6000, S4810, S4820T, S5048F-ON, MXL, FN-IOM, and C9010.

**Usage Information** When you upgrade the Dell EMC Networking OS from an earlier version to 9.14.1.3 or later, the system converts the DHCP CONFIGURATION `host` command in the running configuration to the `host-address` command. If you downgrade the Dell EMC Networking OS from version 9.14.1.3 or later to an earlier version, any existing `host-address` command is deleted from the running configuration. If you want to create manual DHCP bindings, use the `host` command.

## ip dhcp server

Enable DHCP server globally.

**Syntax** `[no] ip dhcp server`  
To disable the DHCP server, use the `no ip dhcp server` command.

**Defaults** Disabled

**Command Modes** CONFIGURATION

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

Version	Description
9.12(1.0)	Introduced on the S5048F-ON.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the S4810 and S4820T.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

## lease

Specify a lease time for the addresses in a pool.

**Syntax** `lease {days [hours] [minutes] | infinite}`

<b>Parameters</b>	<b>days</b>	Enter the number of days of the lease. The range is from 0 to 31.
	<b>hours</b>	Enter the number of hours of the lease. The range is from 0 to 23.
	<b>minutes</b>	Enter the number of minutes of the lease. The range is from 0 to 59.
	<b>infinite</b>	Specify that the lease never expires.

**Defaults** 24 hours

**Command Modes** DHCP <POOL>

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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]

<b>Parameters</b>	<b>address</b>	Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.
-------------------	----------------	--

**Defaults** none

**Command Modes** DHCP <POOL>

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking Operating System (OS) recommends specifying clients as hybrid.

**Syntax** netbios-node-type type

<b>Parameters</b>	<b>type</b>	Enter the NETBIOS node type: <ul style="list-style-type: none"> <li>• Broadcast: Enter the keyword b-node.</li> <li>• Hybrid: Enter the keyword h-node.</li> <li>• Mixed: Enter the keyword m-node.</li> <li>• Peer-to-peer: Enter the keyword p-node.</li> </ul>
-------------------	-------------	---

**Defaults** Hybrid

**Command Modes** DHCP <POOL>

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## network

Specify the range of addresses in an address pool.

<b>Syntax</b>	<code>network network /prefix-length</code>	
<b>Parameters</b>	<b><i>network/ prefix-length</i></b>	Specify a range of addresses. Prefix-length range is from 17 to 31.
<b>Defaults</b>	none	
<b>Command Modes</b>	DHCP <POOL>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip dhcp binding

Display the DHCP binding table.

<b>Syntax</b>	<code>show ip dhcp binding</code>	
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip dhcp configuration

Display the DHCP configuration.

<b>Syntax</b>	<code>show ip dhcp configuration [global   pool name]</code>	
<b>Parameters</b>	<b><i>pool name</i></b>	Display the configuration for a DHCP pool.
	<b><i>global</i></b>	Display the DHCP configuration for the entire system.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip dhcp conflict

Display the address conflict log.

<b>Syntax</b>	<code>show ip dhcp conflict address</code>	
<b>Parameters</b>	<b>address</b>	Display a particular conflict log entry.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip dhcp server

Display the DHCP server statistics.

<b>Syntax</b>	<code>show ip dhcp server statistics</code>	
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

# Commands to Configure the System to be a DHCP Client

To configure the system to be a DHCP client, use the following commands.

## ip address dhcp

Acquire an IP address dynamically on an interface from the DHCP server.

<b>Syntax</b>	<code>ip address dhcp [relay   vendor-class-identifier]</code>	
	To disable DHCP Client on an interface, use the <code>no ip address dhcp</code> command.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	All Modes	
<b>Default</b>	Enabled	



<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	In the I/O Aggregator, the DHCP client is enabled only on the default VLAN and management interface 0/0. Use the <code>ip address</code> command to assign a static IP address that overwrites the dynamically assigned IP address.	

## Other Commands Supported by the DHCP Client

The following commands are supported by the DHCP client.

### clear ip dhcp client statistics

Displays DHCP client statistics, including the number of DHCP messages sent and received on an interface.

<b>Syntax</b>	<code>clear ip dhcp client statistics interface <i>type slot/port</i></code>	
<b>Parameters</b>	<b>interface <i>type slot/port</i></b>	Clear DHCP client statistics on the specified interface. <ul style="list-style-type: none"> <li>For the management interface on the stack-unit, enter the keyword <code>managementethernet</code> followed by slot/port information. The slot and port range is 0.</li> <li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li> </ul>
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Default</b>	None	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### debug ip dhcp client events

Enable the display of log messages for the following events on DHCP client interfaces:

- IP address acquisition
- IP address release
- Renewal of IP address and lease time
- Release of an IP address

<b>Syntax</b>	<code>debug ip dhcp client events [<i>interface type slot/port</i>]</code>	
<b>Parameters</b>	<b>interface <i>type slot/port</i></b>	Display log messages for DHCP packets sent and received on the specified interface. <ul style="list-style-type: none"> <li>For the management interface on the stack-unit, enter the keyword <code>managementethernet</code> followed by slot/port information. The slot and port range is 0</li> <li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li> </ul>

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** None

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## debug ip dhcp client packets

Enable the display of log messages for all DHCP packets sent and received on DHCP client interfaces.

**Syntax** `debug ip dhcp client packets [interface type slot/port]`

**Parameters**

<b>interface type slot/port</b>	
	Display log messages for DHCP packets sent and received on the specified interface.
	<ul style="list-style-type: none"><li>For the management interface on the stack-unit, enter the keyword <code>managementethernet</code> followed by slot/port information. The slot and port range is 0</li><li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li></ul>

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** None

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## release dhcp interface

Release the dynamically-acquired IP address on an Ethernet interface while retaining the DHCP client configuration on the interface.

**Syntax** `release dhcp interface type slot/port`

**Parameters**

<b>interface type slot/port</b>	
	<ul style="list-style-type: none"><li>For the management interface on the stack-unit, enter the keyword <code>management ethernet</code> followed by slot/port information. The slot and port range is 0.</li><li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li></ul>

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** None

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

Version	Description
9.2(0.0)	Supported on the M I/O Aggregator.

**Usage Information**

When you enter the `release dhcp` command, although the IP address that was dynamically-acquired from a DHCP server is released from an interface, the ability to acquire a new DHCP server-assigned address remains in the running configuration for the interface. To acquire a new IP address, enter either the `renew dhcp` command at the EXEC privilege level or the `ip address dhcp` command at the interface configuration level.

## renew dhcp interface

Re-acquire a dynamic IP address on an Ethernet interface enabled as a DHCP client.

**Syntax** `renew dhcp interface type slot/port`

**Parameters**

**interface type slot/port** Enter any of the following keywords and slot/port or number to clear counters from a specified interface:

- For the management interface on the stack-unit, enter the keyword `managementethernet` followed by slot/port information. The slot and port range is 0.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** None.

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage information**

The `renew dhcp` command is used to renew the lease of IP address obtained through dhcp. To display the currently configure dynamic IP address and lease time, enter the `show ip dhcp lease` command.

## show ip dhcp client statistics

Displays DHCP client statistics, including the number of DHCP messages sent and received on an interface.

**Syntax** `show ip dhcp client statistics interface type slot/port`

**Parameters**

**interface type slot/port** Display DHCP client statistics on the specified interface.

- For the management interface on the stack-unit, enter the keyword `managementethernet` followed by slot/port information. The slot and port range is 0.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** None.

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## show ip dhcp lease

Displays lease information about the dynamic IP address currently assigned to a DHCP client-enabled interface.

**Syntax** `show ip dhcp lease [interface type slot/port]`

**Parameters**

<b>interface type</b> <b>slot/port</b>	Display DHCP client statistics on the specified interface. <ul style="list-style-type: none"> <li>For the management interface on the stack-unit, enter the keyword <code>managementethernet</code> followed by slot/port information. The slot and port range is 0.</li> <li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li> </ul>
---	---

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Default** Display DHCP lease information on all DHCP client-enabled interfaces on the switch.

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [arp inspection-trust](#) — specifies a port as trusted so that ARP frames are not validated against the binding table.

## arp inspection-limit

Configure dynamic ARP inspection rate-limit to verify the rate of ARP packet received in a port on a specific interval.

<b>Syntax</b>	<code>arp inspection-limit {rate <i>pps</i> [interval <i>seconds</i>]}</code>	
<b>Defaults</b>	None	
<b>Command Modes</b>	INTERFACE CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Parameters</b>	<b>rate <i>pps</i></b>	Enter the keyword <code>rate</code> then the packet per second (pps) value. The range is from 1 to 2048. The default is 15.
	<b>interval <i>seconds</i></b>	(Optional) Enter the keyword <code>interval</code> then the burst interval in seconds. The range is from 1 to 15. The default is 1.
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .	
	<b>Version</b>	<b>Description</b>
	<b>9.14(1.0)</b>	Introduced on the S3048-ON, S4048-ON, S4048T-ON, S3100 Series, Z9100-ON, S6100-ON, S6000, S6000-ON, S6010-ON, S5048F-ON, S4810, S4820T, FN IOM and MXL.

## arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

<b>Syntax</b>	<code>arp inspection-trust</code>	
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	<ul style="list-style-type: none"><li>• INTERFACE</li><li>• INTERFACE PORT-CHANNEL</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">arp inspection</a> — enables dynamic ARP inspection on a VLAN.	

## clear ip dhcp snooping

Clear the DHCP binding table.

<b>Syntax</b>	<code>clear ip dhcp snooping binding</code>	
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes**        Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM

### Example

```
Dell# clear ipv6 dhcp snooping?
binding    Clear the snooping binding database
```

## ip dhcp relay source-interface

Configure IPv4 DHCP relay source interface.

**Syntax**                    `ip dhcp relay source-interface interface`

To disable the IPv4 DHCP relay source interface, use the `no ip dhcp relay source-interface interface` command.

### Parameters

- |  |  |
|--|--|
| <b>source-interface <i>interface</i></b> | Enter the keyword <code>source-interface</code> then the type of interface and the interface information: <ul style="list-style-type: none"><li>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> then the slot/plot information.</li><li>• For a 10-Gigabit Ethernet information, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For a 40-Gigabit Ethernet information, enter the keyword <code>FortyGigabitEthernet</code> then the slot/port information.</li><li>• For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li><li>• For a Tunnel interface, enter the keyword <code>tunnel</code> then the tunnel ID. The range is from 1 to 16383.</li><li>• For a port channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul> |
|--|--|

**Defaults**                    Disabled

**Command Modes**          • CONFIGURATION  
                                • INTERFACE

**Supported Modes**        Full-Switch

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

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON, and Z9100-ON.

**Related Commands**

- [ipv6 dhcp relay source-interface](#)— Configure DHCP relay source IPv6 interface.

## ipv6 dhcp relay source-interface

Configure DHCP relay source IPv6 interface.

**Syntax**

`ipv6 dhcp relay source-interface interface`

To disable the DHCP relay source IPv6 interface, use the `no ipv6 dhcp relay source-interface interface` command.

**Parameters**

<b>source-interface <i>interface</i></b>	Description
	Enter the keyword <code>source-interface</code> then the type of interface and the interface information: <ul style="list-style-type: none"> <li>• For a 1-Gigabit Ethernet interface, enter the keyword <code>GigabitEthernet</code> then the slot/port information.</li> <li>• For a 10-Gigabit Ethernet information, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a 40-Gigabit Ethernet information, enter the keyword <code>FortyGigabitEthernet</code> then the slot/port information.</li> <li>• For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li> <li>• For a Tunnel interface, enter the keyword <code>tunnel</code> then the tunnel ID. The range is from 1 to 16383.</li> <li>• For a port channel interface, enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>

**Defaults**

Disabled

**Command Modes**

- CONFIGURATION
- INTERFACE

**Supported Modes**

Full-Switch

**Command History**

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

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON, and Z9100-ON.

**Related Commands**

- [ip dhcp relay source-interface](#)— Configure DHCP relay source IP interface.

## ip dhcp snooping

Enable DHCP snooping globally.

**Syntax** `[no] ip dhcp snooping`

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

Introduced in the 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). The Dell Networking OS version 8.2.1.0 extends DHCP Snooping to Layer 2, and you do not have to enable relay agent to snoop on Layer 2 interfaces.

**Related Commands** [ip dhcp snooping vlan](#) — enables DHCP snooping on one or more VLANs.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL.

## ip dhcp snooping database

Delay writing the binding table for a specified time.

**Syntax** `ip dhcp snooping database write-delay minutes`

**Parameters** *minutes* The range is from 5 to 21600.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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** *value* 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

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.7(0.0)	Introduced on the MXL.

## 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 *address*** Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.
- vlan-id *vlan-id*** Enter the keywords `vlan-id` then the VLAN to which the host belongs. The range is from 2 to 4094.
- ip *ip-address*** Enter the keyword `ip` then the IP address that the server is leasing.
- interface *type*** Enter the keyword `interface` then the type of interface to which the host is connected:
  - For a Ten-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`.
- slot/port*** Enter the slot and port number of the interface.
- lease *time*** Enter the keyword `lease` then the amount of time the IP address are leased. The range is from 1 to 4294967295.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.13(0.0)	Enhanced the command to map multiple IP addresses to one MAC address. Enhanced to support DHCP snooping in a VLT setup.

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Instructions** You can map multiple IP addresses to the same MAC address.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip dhcp snooping trust

Configure an interface as trusted.

**Syntax** `[no] ip dhcp snooping trust`

**Defaults** **Untrusted**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 dhcp snooping trust

Configure an interface as trusted for DHCP snooping.

**Syntax** `[no] ipv6 dhcp snooping trust`

To disable dhcp snooping trusted capability on this interface, use the `no ipv6 dhcp snooping trust` command.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.7(0.0)	Introduced on the MXL.

## ip dhcp source-address-validation

Enable the IP Source Guard.

**Syntax** [no] ip dhcp source-address-validation [ipmac]

**Parameters** **ipmac** Enable IP+MAC Source Address Validation.

**Defaults** Disabled

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Allocate at least one FP block to `ipmacacl` before you can enable IP+MAC Source Address Validation.

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 snooping vlan

Enable DHCP Snooping on one or more VLANs.

**Syntax** [no] ip dhcp snooping vlan *name*

**Parameters** ***name*** Enter the name of a VLAN on which to enable DHCP Snooping.


**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## ipv6 dhcp snooping vlan

Enable ipv6 DHCP Snooping on VLAN or range of VLANs.

<b>Syntax</b>	<code>[no] ip dhcp snooping vlan <i>vlan-id</i></code> To disable the ipv6 dhcp snooping on VLAN basis or range of VLAN, use the <code>no ip dhcp snooping vlan &lt;vlan-id&gt;</code> command.	
<b>Parameters</b>	<b><i>vlan-id</i></b>	Enter the name of a VLAN id or list of the VLANs to enable DHCP Snooping.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL.

## ip dhcp relay

Enable Option 82.

<b>Syntax</b>	<code>ip dhcp relay information-option [<i>remote-id</i>   <i>trust-downstream</i>]</code>	
<b>Parameters</b>	<b><i>remote-id</i></b>	Configure the system to enable the remote-id string in option-82.
	<b><i>trust-downstream</i></b>	Configure the system to trust Option 82 when it is received from the previous-hop router.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

<b>Syntax</b>	<code>show ip dhcp snooping [<i>binding</i>   <i>source-address-validation</i>]</code>	
<b>Parameters</b>	<b><i>binding</i></b>	Display the interfaces configured with IP Source Guard.
	<b><i>source-address-validation</i></b>	Display the interfaces configured with IP Source Guard.
<b>Defaults</b>	none	
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [clear ip dhcp snooping](#) — clears the contents of the DHCP binding table.

## show ipv6 DHCP snooping

Display the DHCPv6 snooping database.

**Syntax** `show ipv6 dhcp snooping`

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL.

### 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#
```

## 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** `[no] ip dhcp snooping verify mac-address`

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 DHCP snooping verify mac-address

Configure to enable verify source mac-address against ipv6 DHCP packet 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL.

# Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) is supported on the Dell Networking OS.

## Topics:

- [ecmp-group](#)
- [hash-algorithm](#)
- [hash-algorithm ecmp](#)
- [hash-algorithm seed](#)
- [ip ecmp-group](#)
- [link-bundle-distribution trigger-threshold](#)
- [link-bundle-monitor enable](#)
- [show config](#)
- [show link-bundle distribution](#)

## 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.

<b>Syntax</b>	<code>ecmp-group {<i>ecmp-group-id</i> interface <i>interface</i>   link-bundle-monitor}</code>	
	To remove the selected interface, use the <code>ecmp-group no interface</code> command.	
	To disable link bundle monitoring, use the <code>ecmp-group no link-bundle-monitor</code> command.	
<b>Parameters</b>	<b><i>ecmp-group ID</i></b>	Enter the identifier number for the ECMP group. The range is from 2 to 64.
	<b><i>interface</i></b>	Enter the following keywords and slot/port to add the interface to the ECMP group: <ul style="list-style-type: none"> <li>• 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>
	<b><i>link-bundle-monitor</i></b>	Enter the keywords <code>link-bundle-monitor</code> to enable link bundle monitoring.
<b>Defaults</b>	Off	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONFIGURATION</li> <li>• CONFIGURATION ECMP-GROUP</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a Port Channel.

<b>Syntax</b>	<code>hash-algorithm {<i>algorithm-number</i>   {ecmp {<i>crc16</i>   <i>crc16cc</i>   <i>crc32MSB</i>   <i>crc32LSB</i>   <i>crc-upper</i>   <i>dest-ip</i>   <i>lsb</i>   <i>xor1</i>   <i>xor2</i>   <i>xor4</i>   <i>xor8</i>   <i>xor16</i>}}</code>
---------------	---

```
[number] lag {checksum | crc | xor} [number] nh-ecmp {checksum | crc |
xor}[number] linecard number ip-sa-mask value ip-da-mask value | seed seed-
value }hash-algorithm {ecmp {crc16 | crc16cc | crc32MSB | crc32LSB | crc-
upper | dest-ip | flow-based-hashing {crc16|crc16cc|crc32MSB|crc32LSB|xor1|
xor2|xor4|xor8|xor16}|lsb | xor1 | xor2 | xor4 | xor8 | xor16}[[hg {crc16
| crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4 | xor8 | xor16}]]
[lag {crc16 | crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4 | xor8 |
xor16 }][stack-unit|linecard number | port-set number] | [hg-seed value] |
[seedvalue]
```

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 / line-card, use the `no hash-algorithm linecard number` command.

## Parameters

<b>algorithm-number</b>	Enter the algorithm number. The range is from 0 to 47.
<b>ecmp {crc16   crc16cc   crc32MSB   crc32LSB   crc-upper   dest-ip   lsb   xor1   xor2   xor4   xor8   xor16}</b>	<p>TeraScale and ExaScale Only: Enter the keyword <code>ecmp</code> then one of the following options:</p> <ul style="list-style-type: none"> <li>• <code>crc16</code>: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)</li> <li>• <code>crc16cc</code>: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial</li> <li>• <code>crc32MSB</code>: Use CRC32_UPPER — MSB 16 bits of computed CRC32</li> <li>• <code>crc32LSB</code>: Use CRC32_LOWER — LSB 16 bits of computed CRC32</li> <li>• <code>crc-upper</code>: Uses the upper 32 bits of the key for the hash computation</li> <li>• <code>dest-ip</code>: Uses the destination IP for ECMP hashing</li> <li>• <code>lsb</code>: Returns the LSB of the key as the hash</li> <li>• <code>xor1</code>: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1</li> <li>• <code>xor2</code>: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2</li> <li>• <code>xor4</code>: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4</li> <li>• <code>xor8</code>: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8</li> <li>• <code>xor16</code>: Use CR16 — 16 bit XOR</li> </ul>
<b>lag hash algorithm value</b>	Enter the keyword <code>lag</code> then the LAG hash algorithm value. The range is from 0 to 47.
<b>nh-ecmp hash algorithm value</b>	(OPTIONAL) Enter the keyword <code>nh-ecmp</code> then the ECMP hash algorithm value.
<b>linecard number</b>	(OPTIONAL) Enter the keyword <code>linecard</code> then the linecard slot number.
<b>ip-sa-mask value</b>	(OPTIONAL) Enter the keywords <code>ip-sa-mask</code> then the ECMP/LAG hash mask value. The range is from 0 to FF. The default is <b>FF</b> .
<b>ip-da-mask value</b>	(OPTIONAL) Enter the keywords <code>ip-da-mask</code> then the ECMP/LAG hash mask value. The range is from 0 to FF. The default is <b>FF</b> .
<b>ecmp crc16   crc16cc   crc32MSB   crc32LSB   crc-upper   dest-ip   flow-based-hashing   crc16 crc16cc crc32MSB crc32LSB xor1   xor2   xor4   xor8</b>	<p>Enter the keyword <code>ecmp</code> then one of the following options:</p> <ul style="list-style-type: none"> <li>• <code>crc16</code>: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)</li> <li>• <code>crc16cc</code>: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial</li> <li>• <code>crc32MSB</code>: Use CRC32_UPPER — MSB 16 bits of computed CRC32</li> <li>• <code>crc32LSB</code>: Use CRC32_LOWER — LSB 16 bits of computed CRC32</li> <li>• <code>crc-upper</code>: Uses the upper 32 bits of the key for the hash computation</li> <li>• <code>dest-ip</code>: Uses the destination IP for ECMP hashing</li> <li>• <code>flow-based-hashing</code>: Enter the keywords <code>flow-based-hashing</code> followed by the algorithm</li> </ul>



**| xor16| |lsb |** *crc16 |crc16cc |crc32MSB |crc32LSB |xor1 |xor2 |xor4 |xor8 | xor16*

**xor1 | xor2 | xor4**

**| xor8 | xor16**

- *lsb*: Returns the LSB of the key as the hash
- *xor1*: Use CRC16\_BISYNC\_AND\_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16\_BISYNC\_AND\_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16\_BISYNC\_AND\_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16\_BISYNC\_AND\_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16 bit XOR

**hg {crc16**

**| crc16cc |**

**crc32MSB |**

**crc32LSB | xor1 |**

**xor2 | xor4 | xor8**

**| xor16}**

Enter the keyword **hg** then one of the following options available in the stack-unit and linecard provisioned devices:

- *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

**lag {crc16**

**| crc16cc |**

**crc32MSB |**

**crc32LSB | xor1 |**

**xor2 | xor4 | xor8**

**| xor16}**

Enter the keyword **hg** then one of the following options available in the stack-unit and linecard provisioned devices::

- *crc16*: Use CRC16\_BISYNC — 16 bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16\_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32\_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32\_LOWER — LSB 16 bits of computed CRC32
- *xor1*: Use CRC16\_BISYNC\_AND\_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16\_BISYNC\_AND\_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16\_BISYNC\_AND\_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16\_BISYNC\_AND\_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16 bit XOR

**hg-seed seed-value** (This option is available in stack-unit and linecard provisioned devices): Enter the keywords **hg-seed** then the hash algorithm seed value. The range is from 0 to 2147483646.

**stack-unit number** (OPTIONAL) : Enter the keyword **stack-unit** then the stack-unit slot number.

**linecard number** (OPTIONAL) : Enter the keyword **linecard** then the linecard slot number.

**port-set number** (OPTIONAL) Enter the keyword **port-set** then the port-set slot number.

**Defaults** 0 for hash-algorithm value on TeraScale and ExaScale IPSA and IPDA mask value is **FF** for a line card.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM. Added flow-based-hashing support for hashing on ECMP.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>To ensure that CRC is not used for LAG, set the default hash-algorithm method on ExaScale systems. For example, <code>hash-algorithm ecmp xor lag checksum nh-ecmp checksum</code>.</p> <p>To achieve the functionality of hash-align on the ExaScale platform, do not use CRC as a hash-algorithm method.</p> <p>The hash value calculated with the <code>hash-algorithm</code> command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.</p> <p>The line card option is applicable with the <code>lag-hash-align</code> microcode only (refer to <a href="#">CAM Profile Commands</a>). Any other microcode returns an error message as follows:</p> <ul style="list-style-type: none"> <li>• <code>Dell(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff</code></li> <li>• <code>% Error: This command is not supported in the current microcode configuration</code></li> </ul> <p>In addition, the <code>linecard number ip-sa-mask value ip-da-mask value</code> option has the following behavior to maintain bi-directionality:</p> <ul style="list-style-type: none"> <li>• When hashing is done on both IPSA and IPDA, the <code>ip-sa-mask</code> and <code>ip-da-mask</code> values must be equal. (Single Linecard).</li> <li>• When hashing is done only on IPSA or IPDA, the Dell Networking OS maintains bi-directionality with masks set to <code>XX 00</code> for line card 1 and <code>00 XX</code> for line card 2 (<code>ip-sa-mask</code> and <code>ip-da-mask</code>). The mask value must be the same for both line cards when using multiple line cards as ingress (where <code>XX</code> is any value from <code>00</code> to <code>FF</code> for both line cards). For example, assume that traffic is flowing between linecard 1 and linecard 2:</li> </ul> <ul style="list-style-type: none"> <li>• <code>hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00</code></li> <li>• <code>hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa</code></li> </ul> <p>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 <code>hash-algorithm</code> command to designate another algorithm.</p> <p>When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.</p> <p>On TeraScale, if you do not enter the keyword <code>ECMP</code> or <code>LAG</code>, the Dell Networking OS assumes it to be common for both. If the keyword <code>ECMP</code> or <code>LAG</code> is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for both TeraScale and ExaScale support the range 0-47. The default for ExaScale is <b>24</b>.</p>	

## hash-algorithm ecmp

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

**Syntax** `hash-algorithm ecmp {crc-upper} | {dest-ip} | {lsb}`  
 To return to the default hash algorithm, use the `no hash-algorithm ecmp` command.

**Parameters**

<b>crc-upper</b>	Uses the upper 32 bits of the key for the hash computation. The default is <b>crc-lower</b> .
<b>dest-ip</b>	Uses the destination IP for ECMP hashing. The default is <b>enabled</b> .
<b>lsb</b>	Returns the LSB of the key as the hash. The default is <b>crc-lower</b> .

**Defaults**

- **crc-lower**
- **dest-ip enabled**

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The hash value calculated with the `hash-algorithm` command is unique to the entire chassis. The default ECMP hash configuration is **crc-lower**. This command takes the lower 32 bits of the hash key to compute the egress port and is the “fall-back” configuration if you have not configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, use this command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

## hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

**Syntax** `hash-algorithm seed value [linecard slot] [port-set number]`

**Parameters**

<b>seed value</b>	Enter the keyword <code>seed</code> then the seed value. The range is from 0 to 4095.
<b>linecard slot</b>	Enter the keyword <code>linecard</code> then the linecard slot number.
<b>port-set number</b>	Enter the keywords <code>port-set</code> then the linecard port-pipe number.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This behavior means that for a given flow, even though the prefixes are sorted, two unrelated chassis select different hops.

The Dell Networking OS provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.

**NOTE:** While the seed is stored separately on each port-pipe, the same seed is used across all CAMs. You cannot separate LAG and ECMP but you can use different algorithms across the chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior.

If the hash algorithm configuration is removed, the hash seed does not go to the original factory default setting.

## ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM hold for a route, By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

**Syntax** `ip ecmp-group {maximum-paths | {number} {path-fallback}}`  
To negate a command, use the `no ip ecmp-group maximum-paths` command.

**Parameters**

<b>maximum-paths</b>	Specify the maximum number of ECMP for a route. The range is 2 to 64.
<b>path-fallback</b>	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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You must save the new ECMP settings to the startup-config (`write mem`) then reload the system for the new settings to take effect.

**Related Commands** [show ip cam stack-unit](#) — Display content-addressable memory (CAM) entries.

## 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]`

**Parameters**

<b>percent</b>	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 <b>60%</b> .
----------------	---

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## show config

Display the ECMP configuration.

<b>Syntax</b>	show config
<b>Command Modes</b>	CONFIGURATION-ECMP-GROUP
<b>Supported Modes</b>	Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## show link-bundle distribution

Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

<b>Syntax</b>	show link-bundle-distribution
<b>Command Modes</b>	EXEC Privilege
<b>Supported Modes</b>	Full-Switch

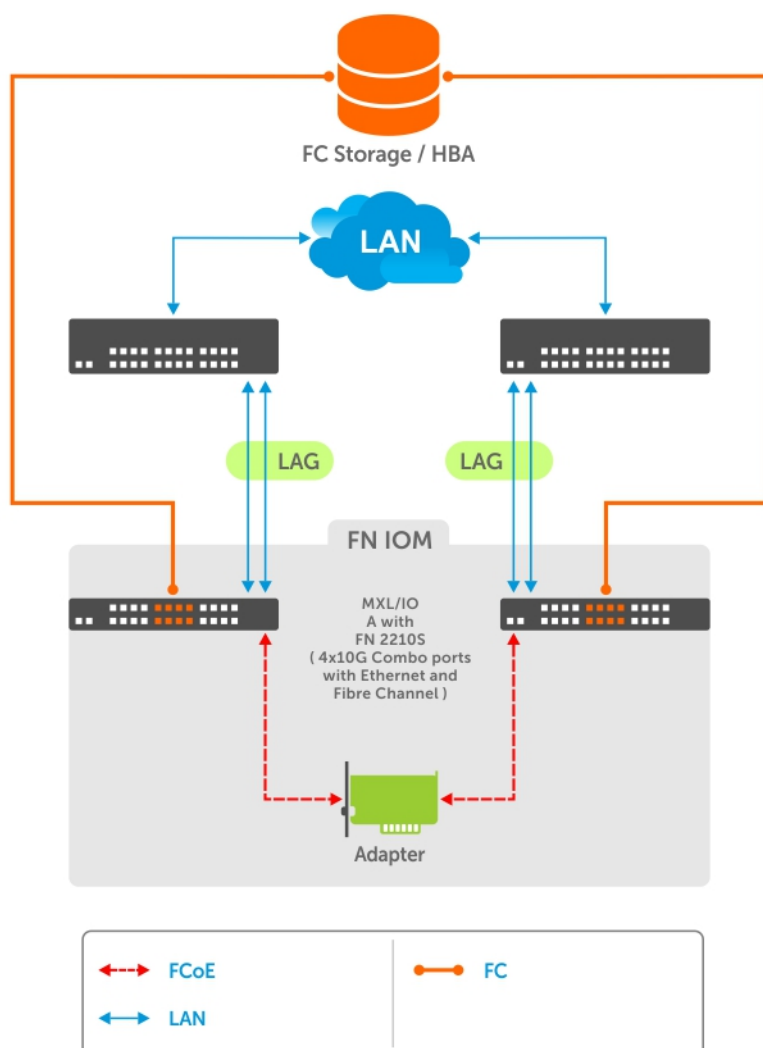
Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show link-bundle-distribution
Link-bundle trigger threshold - 60
ECMP bundle - 5 Utilization[In Percent] - 0 Alarm State - Inactive
Interface Line Protocol Utilization[In Percent]
Te 0/4 Up 5
Te 0/3 Up 30
```

## FC FLEXIO FPORT

The switch is a blade switch which is plugged into the Dell M1000 Blade server chassis. The blade module contains two slots for pluggable flexible module. With single FC Flex IO module, 4 ports are supported, whereas 8 ports are supported with both FC Flex IO modules. Each port can operate in 2G, 4G or 8G Fiber Channel speed. The topology-wise, FC Flex IOM is directly connected to a FC Storage. In the following topology, the FC flex IOM model offers local connectivity without a SAN switch or fabric.



### Topics:

- `feature fc`
- `fc zone`
- `fc alias`
- `fc zoneset`
- `fcoe-map`
- `fabric`
- `active-zoneset`
- `stack-unit port-group port portmode`
- `show fc ns`

- [show fc switch](#)
- [show fc zoneset](#)
- [show fc zone](#)
- [show fc alias](#)
- [show fcoe-map](#)
- [show system stack-unit port-group portmode](#)

## feature fc

Enable feature fc with FPort functionality.

**Syntax** `feature fc fport domain-id range`

**Parameters** **Range** Enter the range from 1 to 239.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Enable `remote-fault-signaling rx off` command in FCF FPort mode on interfaces connected to the Compellent and MDF storage devices.

**Example**

```
Dell(conf)#feature fc fport domain-id
```

## fc zone

Create a zone.

**Syntax** `fc zone zonename member`

To delete a zone, use the `no fc zone zonename member` command.

**Parameters**

**zonename** Enter the zone name.

**member** Enter the WWPN, port ID, or domain/port.

**Command Modes** ALIAS CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>9.1(1.0)</b>	Introduced on the S5000.

**Example without member**

```
Dell(conf)# fc zone z1
Dell(conf-fc-zone-z1)#
```

**Example with member**

```
Dell(conf)#fc zone test
Dell(conf-fc-zone-test)#member ?
WORD                               WWN(00:00:00:00:00:00:00:00), or
```

```
Alias name(word)
Dell(conf-fc-zone-test)#member
```

### Related Commands

[show fc zone](#) — displays the configured zone.

[show fcoe-map](#) — displays the fabric parameters.

## fc alias

Create a zone alias name.

### Syntax

```
fc alias ZoneAliasName member name
```

To delete a zone alias name, use the `no fc zone ZoneAliasName` command.

### Parameters

**ZoneAliasName** Enter the zone alias name.  
**member name** Enter the WWPN, port ID, or domain/port.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL and IOA.
9.1(1.0)	Introduced on the S5000.

### Example

```
Dell(conf)#fc alias test12
Dell(conf-fc-alias-test12)#?
end                Exit from configuration mode
exit              Exit from Alias config mode
member           Add Alias member
no               Negate a command or set its defaults
show            Show alias profile configuration
Dell(conf-fc-alias-test12)#member ?
WORD             WWN(00:00:00:00:00:00:00:00), or portID(123000)
```

### Related Commands

[show fc alias](#) — displays the configured alias.

## fc zoneset

Create a zoneset.

### Syntax

```
fc zoneset zoneset_name [member]
```

To delete a zoneset, use the `no fc zoneset zoneset_name [member]` command.

### Parameters

**zoneset\_name** Enter the zoneset name.  
**member** Enter the WWPN, FC-ID, or Alias name.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.



Version	Description
9.7(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1(1.0)	Introduced on the S5000.

#### Example

```
Dell(conf)#fc zoneset test1
Dell(conf-fc-zoneset-test1)#member ?
WORD Zone Name
Dell(conf-fc-zoneset-test1)#member
```

#### Related Commands

[show fc zoneset](#) — displays the configured and active zoneset.  
[show fcoe-map](#) — displays the fabric parameters.

## fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

<b>Syntax</b>	<code>fcoe-map map-name</code>	
<b>Parameters</b>	<b>map-name</b>	Maximum: 32 alphanumeric characters.
<b>Defaults</b>	None	
<b>Command Modes</b>	CONFIGURATION INTERFACE	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
	9.0(1.3)	Introduced on the S5000.


#### Usage Information

An FCoE map is a template to map FCoE and FC parameters in a converged fabric. An FCoE map virtualizes upstream FC ports on an NPIV proxy gateway to appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network. It provides necessary parameters to FCoE-enabled servers and switches to log in to a SAN fabric.

On an FN IOM NPIV proxy gateway, an FCoE map is applied on fabric-facing FC ports and server-facing Ethernet ports. Use the `fcoe-map` command to apply an FCoE map on an Ethernet port. Use the `fabric` command to apply an FCoE map on an FC port.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority, and the FIP keepalive (FKA) advertisement timeout.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map map-name` command in Interface configuration mode.

 **NOTE:** In FCF F mode, you can create only 1 FCoE map. It doesn't get created automatically. If you try to create more than 1 map, an error message is displayed.

#### Related Commands

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

# fabric

Apply an FCoE map on a fabric-facing Fibre Channel (FC) port.

<b>Syntax</b>	<code>fabric map-name</code>
<b>Parameters</b>	<b>map-name</b> Maximum: 32 alphanumeric characters.
<b>Defaults</b>	None
<b>Command Modes</b>	INTERFACE FIBRE_CHANNEL
<b>Supported Modes</b>	Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>9.0(1.3)</b>	Introduced on the S5000.

**Usage Information** An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map virtualizes the upstream FC ports on an NPIV proxy gateway to appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network. It provides necessary parameters to FCoE-enabled servers and switches to log in to a SAN fabric. Use the `fcoe-map` command to create an FCoE map.

On an FN IOM NPIV proxy gateway, an FCoE map is applied on fabric-facing FC ports and server-facing Ethernet ports. Use the `fabric` command to apply an FCoE map on an FC port. Use the `fcoe-map` command to apply an FCoE map on an Ethernet port.

After you apply an FCoE map on an FC interface, when the port is enabled (`no shutdown`), the NPIV proxy gateway starts sending FIP multicast advertisements on behalf of the FC port to downstream servers to advertise the availability of a new FCF port on the FCoE VLAN.

To remove an FCoE map from an FC interface, enter the `no fabric map-name` command in Interface configuration mode.

**Related Commands** [fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.  
[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

# active-zoneset

Activate the zoneset.

<b>Syntax</b>	<code>active-zoneset zoneset_name</code>
	To change to the default zone behavior, use the <code>no active-zoneset zoneset_name</code> command.

**Parameters** **zoneset\_name** Enter the zoneset name.

**Command Modes** FC FABRIC CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>9.1(1.0)</b>	Introduced on the S5000.

## Example

```
Dell(conf)# fcoe-map default_full_fabric
Dell(conf-fcoe-default_full_fabric)# fc-fabric
Dell(conf-fmap-default_full_fabric-fcfabric)# active-zoneset zs1
```

## Related Commands

[show fc zoneset](#) — displays the configured and active zoneset.

# stack-unit port-group port portmode

Convert the external ports to Fibre Channel or Ethernet mode.

**Syntax** `stack-unit unit number port-group 0-1 port 9-12 portmode {ethernet | fc}`

<b>Parameters</b>	<b>stack-unit</b>	Enter the keywords <code>stack-unit</code> then the stack member number to select the stack unit. The range is from 0 to 5.
	<b>port-group</b>	Enter the keywords <code>port-group</code> then the port group number. The range is from 0 to 1.
	<b>port</b>	Enter the keyword <code>port</code> then the port number. The range is from 9 to 12. The port numbers 9 to 10 map to port-group 0 and the port numbers 11 to 12 map to port-group 1.
	<b>portmode</b>	Enter the keyword <code>portmode</code> to set the port mode. The options are: <ul style="list-style-type: none"><li>• <code>ethernet</code> – convert to Ethernet mode.</li><li>• <code>fc</code> – convert to Fibre Channel mode.</li></ul>

**Defaults** Ports 9, 10 – Fibre Channel mode  
Ports 11, 12 – Ethernet mode

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

## Command History

Version	Description
9.11(0.0)	Included support for all external ports.
9.6(0.0)	Supported on the FN2210S Aggregator.

## Related Commands

[show system stack-unit port-group portmode](#) — displays the port-group port mode information.

# show fc ns

Display the devices in the name server database.

**Syntax** `show fc ns { switch } [brief]`

<b>Parameters</b>	<b>switch</b>	Enter the keyword <code>switch</code> to display all the devices in the name server database of the switch.
	<b>brief</b>	Enter the keyword <code>brief</code> to display in brief devices in the name server database.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1(1.0)	Introduced on the S5000.

## Example

```
Dell#show fc ns switch
Total number of devices = 1
Switch Name                10:00:5c:f9:dd:ef:0a:00
Domain Id                  1
Switch Port                53
Port Id                    01:35:00
Port Name                  10:00:8c:7c:ff:17:f8:01
Node Name                  20:00:8c:7c:ff:17:f8:01
Class of Service          8
IP Address
Symbolic Port Name        Brocade-1860 | 3.0.3.0 | DV-SP-SERVER2 |
|
Symbolic Node Name        (NULL)
Port Type                  Node port
Registered with NameServer Yes
Registered for SCN        Yes
Display of local name server entries - brief version
Dell#

Dell#show fc ns switch brief
Total number of devices = 1
Intf#   Domain  FC-ID      Enode-WWPN
Enode-WWNN
53      1          01:35:00   10:00:8c:7c:ff:17:f8:01
20:00:8c:7c:ff:17:f8:01
Dell#

Dell#show fc ns fabric
Total number of devices = 3
Switch Name                10:00:5c:f9:dd:ef:0a:80
Domain Id                  2
Switch Port                9
Port Id                    02:09:00
Port Name                  32:11:0e:fc:00:00:00:88
Node Name                  22:11:0e:fc:00:00:00:88
Class of Service          8
IP Address
Symbolic Port Name        (NULL)
Symbolic Node Name        (NULL)
Port Type                  Node port
Registered with NameServer No
Registered for SCN        No
Switch Name                10:00:5c:f9:dd:ef:0a:80
Domain Id                  2
Switch Port                11
Port Id                    02:0b:00
Port Name                  31:11:0e:fc:00:00:00:77
Node Name                  21:11:0e:fc:00:00:00:77
Class of Service          8
IP Address
Symbolic Port Name        (NULL)
Symbolic Node Name        (NULL)
Port Type                  Node port
Registered with NameServer No
Registered for SCN        No
Switch Name                10:00:5c:f9:dd:ef:0a:00
Domain Id                  1
Switch Port                53
Port Id                    01:35:00
Port Name                  10:00:8c:7c:ff:17:f8:01
Node Name                  20:00:8c:7c:ff:17:f8:01
```

```

Class of Service      8
IP Address
Symbolic Port Name   Brocade-1860 | 3.0.3.0 | DV-SP-SERVER2 |
|
Symbolic Node Name    (NULL)
Port Type             Node port
Registered with NameServer Yes
Registered for SCN   Yes
Dell#

Dell#show fc ns fabric brief
Total number of devices = 2
Intf#   Domain   FC-ID           Enode-WWPN
Enode-WWNN
9       2        02:09:00        32:11:0e:fc:00:00:00:88
22:11:0e:fc:00:00:88
11      2        02:0b:00        31:11:0e:fc:00:00:00:77
21:11:0e:fc:00:00:77
Dell#

```

## show fc switch

Display the switch configuration for Fibre Channel capability.

**Syntax** `show fc switch`

**Parameters** None

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>9.0(1.3)</b>	Introduced on the S5000.

**Usage Information** The following table describes the `show fc switch` output shown in the following example.

<b>Switch Mode</b>	Fibre Channel mode of operation of an FN IOM switch.
<b>Switch WWN</b>	Factory-assigned worldwide node (WWN) name of the MXL. The MXL WWN name is not user-configurable.

### Example

```

Dell(conf)#do show fc switch
Switch Mode : FPORT
Switch WWN  : 10:00:aa:00:00:00:00:ac
Dell(conf)#

```

## show fc zoneset

Display the configured and active zoneset.

**Syntax** `show fc zoneset [ zoneset_name | active ]`

**Parameters** **zoneset\_name** Enter the zoneset name to display the zoneset name

**active** Enter the keyword `active` to display the active zonesets.  
**merged** Enter the keyword `merged` to display the merge active zones.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1(1.0)	Introduced on the S5000.

**Example**

```
Dell#show fc zoneset

ZoneSetName          ZoneName          ZoneMember
=====
fcoe_srv_fc_tgt
                    brcd_sanb
                                brcd_cna1_wwpn1
                                sanb_p2tgt1_wwpn

Active Zoneset: fcoe_srv_fc_tgt

ZoneName          ZoneMember
=====
brcd_sanb
                    10:00:8c:7c:ff:21:5f:8d
                    20:02:00:11:0d:03:00:00

Dell#

Dell#show fc zoneset active

Active Zoneset: fcoe_srv_fc_tgt

ZoneName          ZoneMember
=====
brcd_sanb
                    10:00:8c:7c:ff:21:5f:8d
                    20:02:00:11:0d:03:00:00

Dell#
```

**Related Commands**

- [fc zone](#) — creates a zone.
- [fc zoneset](#) — creates a zoneset.
- [active-zoneset](#) — activates the zoneset.

## show fc zone

Display the configured zone.

**Syntax** `show fc zone [zonename]`

**Parameters**

**zonename** Enter the zone name to display the details.

**Command Modes**

- EXEC

- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1(1.0)	Introduced on the S5000.

**Example**

```
Dell#show fc zone

ZoneName                               ZoneMember
=====
brcd_sanb                               brcd_cna1_wwpn1
                                         sanb_p2tgt1_wwpn

Dell#
```

**Related Commands** [fc zone](#) — creates a zone.

## show fc alias

Display the configured alias.

**Syntax** `show fc alias [ZoneAliasName ]`

**Parameters** **ZoneAliasName** Enter the zone alias name to display the details.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1(1.0)	Introduced on the S5000.

**Example**

```
Dell#show fc alias

Zone Alias Name      all
0x030303

Dell#
```

**Related Commands** [fc alias](#) — creates a zone alias name.

## show fcoe-map

Display the Fibre Channel and FCoE configuration parameters in FCoE maps.

**Syntax** `show fcoe-map`

**Parameters** None

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
9.1.1.0	Introduced on the S5000.

**Usage Information**

Use the `show fcoe-map` command to display the FC and FCoE parameters used to configure server-facing Ethernet (FCoE) and fabric-facing FC ports in all FCoE maps on the switch.

In each FCoE map, the values for the fabric ID and FC-MAP that identify the SAN fabric to which FC storage traffic is sent, and the FCoE VLAN to be used must be unique.

An FCoE map is used to identify the SAN fabric to which FCoE storage traffic is sent. It also virtualizes the switch with FC Flex IO module FC ports, so that they appear to downstream server CNA ports as FCoE Forwarder (FCF) ports on an FCoE network.

**Example**

```
Dell#show system stack-unit 0 iom-mode
Unit      Boot-Mode          Next-Boot
-----
0         standalone        standalone
Dell#show fcoe-map

Fabric Name          SAN_FABRIC

Fabric Type          npiv
Fabric Id            1002
Vlan Id              1002
Vlan priority        3
FC-MAP               0efc00
FKA-ADV-Period       8
Fcf Priority          128
Config-State         ACTIVE
Oper-State           DOWN
=====
Members
Fc 0/9 Fc 0/10
=====
Dell#
```

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

## show system stack-unit port-group portmode

Display the port-group port mode information.

**Syntax** `show system stack-unit unit-number port-group portmode`

**Parameters** **stack-unit unit-number** Enter the keywords `stack-unit` then the unit number. The range is from 0 to 11.

- Command Modes**
- EXEC
  - EXEC Privilege

**Command History**

Version	Description
9.11(0.0)	Included support for all external ports.



Version	Description
9.6(0.0)	Supported on the FN2210S Aggregator.

**Example**

```
Dell#show system stack-unit 0 port-group portmode
PortGroupId      Ports      Mode(Curr Boot) Mode(Next Boot)
0                9         FC             FC
0                10        FC             FC
1                11        ETH            ETH
1                12        FC             FC
Dell#
```

**Related Commands**

[stack-unit port-group port portmode](#) — converts the external ports to Fibre Channel or Ethernet mode.

# FIPS Cryptography

To configure federal information processing standards (FIPS) cryptography, use the following commands on the switch.

## Topics:

- [fips mode enable](#)
- [show fips status](#)
- [show ip ssh](#)
- [ssh](#)

## fips mode enable

Enable the FIPS cryptography mode on the platform.

**Syntax** `fips mode enable`  
To disable the FIPS cryptography mode, use the `no fips mode enable` command.

**Default** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell (conf)#fips mode enable
WARNING: Enabling FIPS mode will close all SSH/Telnet connection,
restart those servers, and destroy all configured host keys.
proceed (y/n) ? y
Dell (conf)#
```

**Related Commands** `ssh` — opens an SSH connection specifying the hostname, username, port number, and version of the SSH client.

## show fips status

Displays the status of the FIPS mode.

**Syntax** `show fips status`

**Defaults** None

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show fips status
FIPS Mode      : Disabled
Dell#

Dell#show fips status
FIPS Mode      : Enabled
Dell#
```

## show ip ssh

Display information about established SSH sessions

**Syntax** show ip ssh

**Defaults** none

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA Authentication        : disabled.
Vty      Encryption      HMAC      Remote IP
1         3des-cbc       hmac-md5 10.1.20.48
2         3des-cbc       hmac-md5 10.1.20.48
```

### With FIPS Mode enabled:

```
Dell#show ip ssh
SSH server                : enabled.
SSH server version        : v2.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA Authentication        : disabled.
Vty      Encryption      HMAC      Remote IP
0         aes128-cbc     hmac-sha1 10.11.8.13
1         aes128-cbc     hmac-sha1 10.1.20.48
```

## ssh

Open an SSH connection specifying the hostname, username, port number, and version of the SSH client.

**Syntax** ssh {hostname | ipv4 address | ipv6 address} [-c encryption cipher | -l username | -m HMAC algorithm | -p port-number | -v {1|2}]

**Parameters**

<b>hostname</b>	(OPTIONAL) Enter the IP address or the hostname of the remote device.
<b>ipv4 address</b>	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
<b>ipv6 address</b>	(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
<b>prefix-length</b>	

**i** | **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**-c encryption cipher**

Enter the following encryption cipher to use. (For v2 clients only.) Without the FIPS mode enabled:

- `3des-cbc`: Force ssh to use 3des-cbc encryption cipher.

With the FIPS mode enabled:

- `aes128-cbc`: Force ssh to use the aes128-cbc encryption cipher.
- `aes256-cbc`: Force ssh to use the aes256-cbc encryption cipher.

**-l username**

(OPTIONAL) Enter the keyword `-l` then the user name used in this SSH session. The default is the user name of the user associated with the terminal.

**-m HMAC algorithm**

Enter one of the following HMAC algorithms to use. (For v2 clients only.):

Without the FIPS mode enabled:

- `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm.
- `hmac-sha1-96`: Force ssh to use the hmac-sha1-96 HMAC algorithm.
- `hmac-md5`: Force ssh to use the hmac-md5 HMAC algorithm.
- `hmac-md5-96`: Force ssh to use the hmac-md5-96 HMAC algorithm.

With the FIPS mode enabled:

- `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm.
- `hmac-sha1-96`: Force ssh to use the hmac-sha1-96 HMAC algorithm.

**-p port-number**

(OPTIONAL) Enter the keyword `-p` then the port number.

The range is 1 to 65536

The default is 22

**-v {1|2}**

(OPTIONAL) Enter the keyword `-v` then the SSH version 1 or 2.

The default: The version from the protocol negotiation.

**i** | **NOTE:** If the FIPS mode is enabled, this option does not display in the output.

**Defaults** As indicated above.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example** **If FIPS mode is not enabled:**

```
Dell#ssh 10.11.8.12 ?
-c          Encryption cipher to use (for v2 client
-l          User name option
-m          HMAC algorithm to use (for v2 clients only)
-p          SSH server port option (default 22)
-v          SSH protocol version
<cr>
Dell#ssh 10.11.8.12 -c ?
3des-cbc   Force ssh to use 3des-cbc encryption cipher
Dell#ssh 10.11.8.12 -m ?
hmac-sha1  Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5   Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96 Force ssh to use hmac-md5-96 HMAC algorithm
```

**With FIPS mode enabled:**

```
Dell#ssh 10.11.8.12 ?
-c          Encryption cipher to use (for v2 client
-l          User name option
-m          HMAC algorithm to use (for v2 clients only)
-p          SSH server port option (default 22)
<cr>
Dell#ssh 10.11.8.12 -c ?
aes128-cbc  Force ssh to use aes128-cbc encryption cipher
aes256-cbc  Force ssh to use aes256-cbc encryption cipher
Dell#ssh 10.11.8.12 -m ?
hmac-sha1   Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
```

## FIP Snooping

In a converged Ethernet network, an Aggregator can operate as an intermediate Ethernet bridge to snoop on Fibre Channel over Ethernet Initialization Protocol (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 ACLs to permit only authorized FCoE traffic to be transmitted between an FCoE end-device and an FCF.

This chapter describes the FIP snooping commands.

### Topics:

- [clear fip-snooping database interface vlan](#)
- [show fip-snooping statistics](#)
- [debug fip-snooping](#)
- [show fip-snooping config](#)
- [show fip-snooping enode](#)
- [show fip-snooping fcf](#)
- [show fip-snooping sessions](#)
- [show fip-snooping statistics](#)
- [show fip-snooping system](#)
- [show fip-snooping vlan](#)

## clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs FIP snooping generates.

**Syntax** `clear fip-snooping database interface vlan vlan-id {fcoe-mac-address | enode-mac-address | fcf-mac-address}`

**Parameters**

<b><i>fcoe-mac-address</i></b>	Enter the FCoE MAC address to be cleared of FIP snooping information.
<b><i>enode-mac-address</i></b>	Enter the ENode MAC address to be cleared of FIP snooping information.
<b><i>fcf-mac-address</i></b>	Enter the FCF MAC address to be cleared of FIP snooping information.

**Command Modes** EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear fip-snooping statistics

Clear the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

**Syntax** `clear fip-snooping statistics [interface vlanVlan-id| interfaceport-type port/slot|interface port-channel port-channel-number]`

**Parameters**

<b>vlan-id</b>	Enter the VLAN ID of the FIP packet statistics to be cleared.
<b>port type port/slot</b>	Enter the port-type and slot number of the FIP packet statistics to be cleared.
<b>port-channel-number</b>	Enter the port channel number of the FIP packet statistics to be cleared.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## feature fip-snooping

Enable FCoE transit and FIP snooping on a switch.

**Syntax** `feature fip-snooping`  
To disable the FCoE transit feature, use the `no feature fip-snooping` command.

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

**Syntax** `fip-snooping enable`  
To disable the FIP snooping feature on all or a specified VLAN, use the `no fip-snooping enable` command.

**Defaults** FIP snooping is disabled on all VLANs.

**Command Modes** • CONFIGURATION

- VLAN INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>fip-snooping fc-map fc-map-value</code>	
	To return the configured FM-MAP value to the default value, use the <code>no fip-snooping fc-map</code> command.	
<b>Parameters</b>	<b><i>fc-map-value</i></b>	Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.
<b>Defaults</b>	<b>0x0EFC00</b>	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONFIGURATION</li> <li>• VLAN INTERFACE</li> </ul>	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

<b>Syntax</b>	<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.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The maximum number of FCFs supported per FIP snooping-enabled VLAN is four.

## show fip-snooping statistics

Displays 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 | interface port-channel port-channel-number]`

**Parameters**

- vlan-id*** Enter the VLAN ID of the FIP packet statistics to be displayed.
- port-type port/slot*** Enter the port-type and slot number of the FIP packet statistics to be displayed.
- port-channel-number*** Enter the port channel number of the FIP packet statistics to be displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information**

The following table describes the `show fip-snooping statistics` command.

Field	Description
<b>Number of Vlan Requests</b>	Number of FIP-snooped VLAN request frames received on the interface.
<b>Number of VLAN Notifications</b>	Number of FIP-snooped VLAN notification frames received on the interface
<b>Number of Multicast Discovery Solicits</b>	Number of FIP-snooped multicast discovery solicit frames received on the interface.
<b>Number of Unicast Discovery</b>	Number of FIP-snooped unicast discovery solicit frames received on the interface.
<b>Number of FLOGI</b>	Number of FIP-snooped FLOGI request frames received on the interface.
<b>Number of FDISC</b>	Number of FIP-snooped FDISC request frames received on the interface
<b>Number of FLOGO</b>	Number of FIP-snooped FLOGO frames received on the interface
<b>Number of ENode Keep Alives</b>	Number of FIP-snooped ENode keep-alive frames received on the interface

Field	Description
<b>Number of VN Port Keep Alives</b>	Number of FIP-snooped VN port keep-alive frames received on the interface
<b>Number of Multicast Discovery Advertisements</b>	Number of FIP-snooped multicast discovery advertisements received on the interface
<b>Number of Unicast Discovery Advertisements</b>	Number of FIP-snooped unicast discovery advertisements received on the interface
<b>Number of FLOGI Accepts</b>	Number of FIP FLOGI accept frames received on the interface
<b>Number of FLOGI Rejects</b>	Number of FIP FLOGI reject frames received on the interface
<b>Number of FDISC Accepts</b>	Number of FIP FDISC accept frames received on the interface
<b>Number of FDISC Rejects</b>	Number of FIP FDISC reject frames received on the interface
<b>Number of FLOGO Accepts</b>	Number of FIP FLOGO accept frames received on the interface
<b>Number of FLOGO Rejects</b>	Number of FIP FLOGO reject frames received on the interface
<b>Number of CVLs</b>	Number of FIP clear virtual link frames received on the interface
<b>Number of FCF Discovery</b>	Number of FCF discovery timeouts that occurred on the interface
<b>Number of VN Port Session</b>	Number of VN port session timeouts that occurred on the interface
<b>Number of Session failures due to Hardware Config</b>	Number of session failures due to hardware configuration that occurred on the interface

### Example

```
Dell# show fip-snooping statistics interface vlan 100
Number of Vlan Requests                :0
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits  :2
Number of Unicast Discovery Solicits    :0
Number of FLOGI                        :2
Number of FDISC                         :16
Number of FLOGO                         :0
Number of Enode Keep Alive              :9021
Number of VN Port Keep Alive            :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                 :2
Number of FLOGI Rejects                 :0
Number of FDISC Accepts                 :16
Number of FDISC Rejects                 :0
Number of FLOGO Accepts                 :0
Number of FLOGO Rejects                 :0
Number of CVL                           :0
Number of FCF Discovery Timeouts         :0
Number of VN Port Session Timeouts      :0
Number of Session failures due to Hardware Config :0
Dell(conf)#
```

```
Dell# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests :1
Number of Vlan Notifications :0
Number of Multicast Discovery Solicits :1
Number of Unicast Discovery Solicits :0
Number of FLOGI :1
Number of FDISC :16
Number of FLOGO :0
Number of Enode Keep Alive :4416
Number of VN Port Keep Alive :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement :0
Number of FLOGI Accepts :0
Number of FLOGI Rejects :0
Number of FDISC Accepts :0
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0
```

### Example (port channel)

```
Dell# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests :0
Number of Vlan Notifications :2
Number of Multicast Discovery Solicits :0
Number of Unicast Discovery Solicits :0
Number of FLOGI :0
Number of FDISC :0
Number of FLOGO :0
Number of Enode Keep Alive :0
Number of VN Port Keep Alive :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts :2
Number of FLOGI Rejects :0
Number of FDISC Accepts :16
Number of FDISC Rejects :0
Number of FLOGO Accepts :0
Number of FLOGO Rejects :0
Number of CVL :0
Number of FCF Discovery Timeouts :0
Number of VN Port Session Timeouts :0
Number of Session failures due to Hardware Config :0
```

## debug fip-snooping

Enable the debug FIP protocol specific messages.

**Syntax** `debug fip-snooping [all | acl | error | ifm | info | ipc | rx { packet-type { all | discovery | virtual-link-instantiation | virtual-link-maintenance | vlan-discovery } { port-channel | tengigabitethernet } } | tx ]`

**Parameters**

- all** Enable all the debug options.
- acl** Enable for ACL specific debugs.
- error** Enable for Error specific debugs.
- ifm** Enable for IFM specific debugs.
- info** Enable for Information specific debugs.
- ipc** Enable for IPC specific debugs.
- rx** Enable for packet receive specific debugs.

<b>packet-type</b>	Specify the packet type. Options are: <ul style="list-style-type: none"> <li>• all</li> <li>• discovery</li> <li>• virtual-link-instantiation</li> <li>• virtual-link-maintenance</li> <li>• vlan-discovery</li> </ul>
<b>all</b>	Enable for all the packet types.
<b>discovery</b>	Enable for FIP discovery solicits (enodes) and adverts (fcf).
<b>virtual-link-instantiation</b>	Enable for flogi, fdisc and flogo packets.
<b>virtual-link-maintenance</b>	Enable for clear virtual link and keepalive packets.
<b>vlan-discovery</b>	Enable for FIP VLAN requests and notifications.
<b>port-channel</b>	Port-channel interface.
<b>tengigabitethernet</b>	TenGigabit Ethernet interface.
<b>tx</b>	Enable for packet transmit specific debugs.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## show fip-snooping config

Displays the FIP snooping status and configured FC-MAP values.

**Syntax** `show fip-snooping config`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

## show fip-snooping enode

Displays 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 be displayed.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following table describes the `show fip-snooping enode` command.

Field	Description
<b>ENode MAC</b>	MAC address of the ENode
<b>ENode Interface</b>	Slot/ port number of the interface connected to the ENode.
<b>FCF MAC</b>	MAC address of the FCF
<b>VLAN</b>	VLAN ID number used by the session
<b>FC-ID</b>	Fibre Channel session ID assigned by the FCF.

**Example**

```
Dell# show fip-snooping enode
Enode MAC          Enode Interface      FCF MAC
VLAN              FC-ID
-----
-----
54:7f:ee:37:34:40  100                  d4:ae:52:1b:e3:cd   Te 0/11
62:00:11
```

## show fip-snooping fcf

Displays 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 be displayed.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following table describes the `show fip-snooping fcf` command.

Field	Description
<b>FCF MAC</b>	MAC address of the FCF
<b>FCF Interface</b>	Slot/ port number of the interface to which the FCF is connected.
<b>VLAN</b>	VLAN ID number used by the session
<b>FC-MAP</b>	FC-MAP value advertised by the FCF.

Field	Description
<b>FKA_ADV_PERIOD</b>	Period of time (in milliseconds) during which FIP keep-alive advertisements are transmitted.
<b>No of ENodes</b>	Number of ENodes connected to the FCF

### 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 128        100     0e:fc:00  4000
1
```

## show fip-snooping sessions

Displays information on FIP-snooped sessions on all VLANs or a specified VLAN, including the ENode interface and MAC address, the FCF interface and MAC address, VLAN ID, FCoE MAC address and FCoE session ID number (FC-ID), worldwide node name (WWNN) and the worldwide port name (WWPN).

**Syntax** `show fip-snooping sessions[interface vlan vlan-id]`

**Parameters** *vlan-id* Enter the *vlan-id* of the specified VLAN to be displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following table describes the `show fip-snooping sessions` command.

Field	Description
<b>ENode MAC</b>	MAC address of the ENode.
<b>ENode Interface</b>	Slot/ port number of the interface connected to the ENode.
<b>FCF MAC</b>	MAC address of the FCF.
<b>FC Interface</b>	Slot/ port number of the interface to which the FCF is connected.
<b>VLAN</b>	VLAN ID number used by the session.
<b>FCoE MAC</b>	MAC address of the FCoE session assigned by the FCF.
<b>FC-ID</b>	Fibre Channel ID assigned by the FCF.
<b>Port WWPN</b>	Worldwide port name of the CNA port.
<b>Port WWNN</b>	Worldwide node name of the CNA port.

### Example

```
Dell#show fip-snooping sessions
Enode MAC          Enode Intf    FCF MAC      FCF Intf  VLAN  FCoE MAC
FC-ID
00:0e:1e:0c:54:a6 Te 0/14 00:05:73:f2:4f:ae Po128 100 0e:fc:00:9a:00:27
9a:00:27 20:01:00:0e:1e:0c:54:a6
00:0e:1e:06:01:5e Te 0/16 00:05:73:f2:4f:af Po128 100 0e:fc:00:9a:01:18
```

```
9a:01:18 20:01:00:0e:1e:06:01:5
Port WWNN
20:00:00:0e:1e:0c:54:a6
20:00:00:0e:1e:0c:54:a6
```

## show fip-snooping statistics

Displays 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 | interface port-channel port-channel-number]`

**Parameters**

<b><i>vlan-id</i></b>	Enter the VLAN ID of the FIP packet statistics to be displayed.
<b><i>port-type port/slot</i></b>	Enter the port-type and slot number of the FIP packet statistics to be displayed.
<b><i>port-channel-number</i></b>	Enter the port channel number of the FIP packet statistics to be displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following table describes the `show fip-snooping statistics` command.

Field	Description
<b>Number of Vlan Requests</b>	Number of FIP-snooped VLAN request frames received on the interface.
<b>Number of VLAN Notifications</b>	Number of FIP-snooped VLAN notification frames received on the interface
<b>Number of Multicast Discovery Solicits</b>	Number of FIP-snooped multicast discovery solicit frames received on the interface.
<b>Number of Unicast Discovery</b>	Number of FIP-snooped unicast discovery solicit frames received on the interface.
<b>Number of FLOGI</b>	Number of FIP-snooped FLOGI request frames received on the interface.
<b>Number of FDISC</b>	Number of FIP-snooped FDISC request frames received on the interface
<b>Number of FLOGO</b>	Number of FIP-snooped FLOGO frames received on the interface
<b>Number of ENode Keep Alives</b>	Number of FIP-snooped ENode keep-alive frames received on the interface
<b>Number of VN Port Keep Alives</b>	Number of FIP-snooped VN port keep-alive frames received on the interface

Field	Description
<b>Number of Multicast Discovery Advertisements</b>	Number of FIP-snooped multicast discovery advertisements received on the interface
<b>Number of Unicast Discovery Advertisements</b>	Number of FIP-snooped unicast discovery advertisements received on the interface
<b>Number of FLOGI Accepts</b>	Number of FIP FLOGI accept frames received on the interface
<b>Number of FLOGI Rejects</b>	Number of FIP FLOGI reject frames received on the interface
<b>Number of FDISC Accepts</b>	Number of FIP FDISC accept frames received on the interface
<b>Number of FDISC Rejects</b>	Number of FIP FDISC reject frames received on the interface
<b>Number of FLOGO Accepts</b>	Number of FIP FLOGO accept frames received on the interface
<b>Number of FLOGO Rejects</b>	Number of FIP FLOGO reject frames received on the interface
<b>Number of CVLs</b>	Number of FIP clear virtual link frames received on the interface
<b>Number of FCF Discovery</b>	Number of FCF discovery timeouts that occurred on the interface
<b>Number of VN Port Session</b>	Number of VN port session timeouts that occurred on the interface
<b>Number of Session failures due to Hardware Config</b>	Number of session failures due to hardware configuration that occurred on the interface

### Example

```

Dell# show fip-snooping statistics interface vlan 100
Number of Vlan Requests                :0
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits  :2
Number of Unicast Discovery Solicits    :0
Number of FLOGI                        :2
Number of FDISC                        :16
Number of FLOGO                        :0
Number of Enode Keep Alive              :9021
Number of VN Port Keep Alive           :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                 :2
Number of FLOGI Rejects                 :0
Number of FDISC Accepts                 :16
Number of FDISC Rejects                 :0
Number of FLOGO Accepts                 :0
Number of FLOGO Rejects                 :0
Number of CVL                           :0
Number of FCF Discovery Timeouts        :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
Dell(conf)#

Dell# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests                :1
Number of Vlan Notifications           :0

```



```

Number of Multicast Discovery Solicits      :1
Number of Unicast Discovery Solicits       :0
Number of FLOGI                            :1
Number of FDISC                            :16
Number of FLOGO                            :0
Number of Enode Keep Alive                 :4416
Number of VN Port Keep Alive               :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement  :0
Number of FLOGI Accepts                   :0
Number of FLOGI Rejects                   :0
Number of FDISC Accepts                   :0
Number of FDISC Rejects                   :0
Number of FLOGO Accepts                   :0
Number of FLOGO Rejects                   :0
Number of CVL                              :0
Number of FCF Discovery Timeouts           :0
Number of VN Port Session Timeouts        :0
Number of Session failures due to Hardware Config :0

```

**Example (port channel)**

```

Dell# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests                      :0
Number of Vlan Notifications                :2
Number of Multicast Discovery Solicits      :0
Number of Unicast Discovery Solicits       :0
Number of FLOGI                            :0
Number of FDISC                            :0
Number of FLOGO                            :0
Number of Enode Keep Alive                 :0
Number of VN Port Keep Alive               :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement  :2
Number of FLOGI Accepts                   :2
Number of FLOGI Rejects                   :0
Number of FDISC Accepts                   :16
Number of FDISC Rejects                   :0
Number of FLOGO Accepts                   :0
Number of FLOGO Rejects                   :0
Number of CVL                              :0
Number of FCF Discovery Timeouts           :0
Number of VN Port Session Timeouts        :0
Number of Session failures due to Hardware Config :0

```

## show fip-snooping system

Displays 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**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 FIP snooping operational VLANs.

**Syntax** `show fip-snooping vlan`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Introduced on the M I/O Aggregator.

### Example

```
Dell# show fip-snooping vlan
* = Default VLAN

VLAN    FC-MAP          FCFs    Enodes    Sessions
----    -
*1      -               -       -         -
1002    0X0EFC00       1       1         1
```

# Force10 Resilient Ring Protocol (FRRP)

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 virtual local area network (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.

### Topics:

- [clear frrp](#)
- [debug frrp](#)
- [description](#)
- [disable](#)
- [interface](#)
- [member-vlan](#)
- [mode](#)
- [protocol frrp](#)
- [show frrp](#)
- [timer](#)

## clear frrp

Clear the FRRP statistics counters.

<b>Syntax</b>	<code>clear frrp [ring-id]</code>	
<b>Parameters</b>	<b>ring-id</b>	(Optional) Enter the ring identification number. The range is from 1 to 255.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN MXL.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>Executing this command without the optional <code>ring-id</code> command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:</p> <ul style="list-style-type: none"> <li>• hello Rx and Tx counters</li> </ul>	

- 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

<b>event</b>	Enter the keyword <code>event</code> to display debug information related to ring protocol transitions.
<b>packet</b>	Enter the keyword <code>packet</code> to display brief debug information related to control packets.
<b>detail</b>	Enter the keyword <code>detail</code> to display detailed debug information related to the entire ring protocol packets.
<b>ring-id</b>	(Optional) Enter the ring identification number. The range is from 1 to 255.
<b>count <i>number</i></b>	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-frrp)

### Supported Modes

Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

```
description Word
```

To remove the ring description, use the `no description [Word]` command.

### Parameters

<b>Word</b>	Enter a description of the ring. Maximum: 255 characters.
-------------	---

<b>Defaults</b>	none	
<b>Command Modes</b>	CONFIGURATION (conf-frpp)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## disable

Disable the resilient ring protocol.

<b>Syntax</b>	<code>disable</code>
	To enable the Resilient Ring Protocol, use the <code>no disable</code> command.

<b>Defaults</b>	<b>Disabled</b>	
<b>Command Modes</b>	CONFIGURATION (conf-frpp)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## interface

Configure the primary, secondary, and control-vlan interfaces.

<b>Syntax</b>	<code>interface {primary <i>interface</i> secondary <i>interface</i> control-vlan <i>vlan-id</i>}</code>
	To return to the default, use the <code>no interface {primary <i>interface</i> secondary <i>interface</i> control-vlan <i>vlan-id</i>}</code> command.

<b>Parameters</b>	<b>primary <i>interface</i></b>	Enter the keyword <code>primary</code> to configure the primary interface then one of the following interfaces and slot/port information: <ul style="list-style-type: none"> <li>Fast Ethernet interface: enter the keyword <code>FastEthernet</code> then the slot/port information.</li> <li>Port Channel interface: enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>10-Gigabit Ethernet interface: enter the keyword <code>TenGigabitEthernet</code> then the slot/port information</li> </ul>
	<b>secondary <i>interface</i></b>	Enter the keyword <code>secondary</code> to configure the secondary interface then one of the following interfaces and slot/port information: <ul style="list-style-type: none"> <li>Fast Ethernet interface: enter the keyword <code>FastEthernet</code> then the slot/port information.</li> <li>Port Channel interface: enter the keyword <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>10-Gigabit Ethernet interface: enter the keyword <code>TenGigabitEthernet</code> then the slot/port information</li> </ul>
	<b>control-vlan <i>vlan-id</i></b>	Enter the keyword <code>control-vlan</code> then the VLAN ID. The range is from 1 to 4094.

<b>Defaults</b>	none
-----------------	------

**Command Modes** CONFIGURATION (conf-frpp)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 frpp](#) — displays the resilient ring protocol configuration information.

## member-vlan

Specify the member VLAN identification numbers.

**Syntax** `member-vlan {vlan-range}`  
To return to the default, use the `no member-vlan [vlan-range]` command.

**Parameters** ***vlan-range*** Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10. Combination: 3, 4, 5-10, 8.

**Defaults** none

**Command Modes** CONFIGURATION (conf-frpp)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## mode

Set the Master or Transit mode of the ring.

**Syntax** `mode {master | transit}`  
To reset the mode, use the `no mode {master | transit}` command.

**Parameters** ***master*** Enter the keyword `master` to set the Ring node to Master mode.  
***transit*** Enter the keyword `transit` to set the Ring node to Transit mode.

**Defaults** Mode None

**Command Modes** CONFIGURATION (conf-frpp)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 `summary` to view just a summarized version of the Ring configuration.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

**Example (Summary)** Dell#show frrp summary

```
Ring-ID State Mode Ctrl_Vlan Member_Vlans
-----
2 UP Master 2 11-20, 25,27-30
31 UP Transit 31 40-41
50 Down Transit 50 32
Dell#
```

### Example (1)

```
Dell#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : TenGigabitEthernet 0/6 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
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 *milliseconds*** Enter the keyword `hello-interval` then the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 milliseconds; for example, 50, 100, 150, and so on. If an invalid value is entered, an error message is generated. The range is from 50 to 2000 ms. Default: **500 ms**.

**dead-interval *milliseconds*** Enter the keyword `dead-interval` then the time, in milliseconds, to set the dead interval of the control packets. The range is from 50 to 6000 ms. Default: **1500 ms**.



**NOTE:** The configured dead interval must be at least three times the hello interval.

### Defaults

- **500 ms** for `hello-interval milliseconds`
- **1500 ms** for `dead-interval milliseconds`

**Command Modes** CONFIGURATION (conf-frrp)

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 (OS) supports the basic GVRP commands.

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 virtual local area network (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 network interface controller (NICs).
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If you enable GVRP, a port that changes to the STP Forwarding state automatically begin to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge must classify and analyze packets by VLAN protocols, manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge must know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

### Topics:

- [clear gvrp statistics](#)
- [debug gvrp](#)
- [disable](#)
- [garp timers](#)
- [gvrp enable](#)
- [gvrp registration](#)
- [protocol gvrp](#)

- [show config](#)
- [show garp timers](#)
- [show gvrp](#)
- [clear gvrp statistics](#)
- [show vlan](#)

## clear gvrp statistics

Clear GVRP statistics on an interface.

**Syntax** `clear gvrp statistics interface interface`

**Parameters**

<b>interface</b>	Enter the following keywords and slot/port or number information:
<b>interface</b>	<ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

<b>config</b>	Enter the keyword <code>config</code> to enable debugging on the GVRP configuration.
<b>event</b>	Enter the keyword <code>event</code> to enable debugging on the JOIN/LEAVE events.
<b>pdu</b>	Enter the keyword <code>pdu</code> then one of the following Interface keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>

**Defaults** Disabled.

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# disable

Globally disable GVRP.

**Syntax** `disable`  
To re-enable GVRP, use the `no disable` command.

**Defaults** Enabled.

**Command Modes** CONFIGURATION-GVRP

**Supported Modes** Full-Switch




Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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		
<b>join</b>	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 <b>200 milliseconds</b> .  <b>NOTE:</b> Designate the milliseconds in multiples of 100.	
<b>leave</b>	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 <b>600 milliseconds</b> .  <b>NOTE:</b> Designate the milliseconds in multiples of 100.	
<b>leave-all</b>	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.  <b>NOTE:</b> Designate the milliseconds in multiples of 100.	

**Defaults** As above.

**Command Modes** CONFIGURATION-GVRP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes**      Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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	normal	forbidden
	Enter the keyword <code>fixed</code> then the VLAN range in a comma-separated VLAN ID set.	Enter the keyword <code>normal</code> then the VLAN range in a comma-separated VLAN ID set. This setting is the default.	Enter the keyword <code>forbidden</code> then the VLAN range in a comma-separated VLAN ID set.

**Defaults**                 **normal**

**Command Modes**        CONFIGURATION-INTERFACE

**Supported Modes**      Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** Full-Switch

### Command History

#### Version

#### Description

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

### Related Commands

[disable](#) — globally disables GVRP.

## show config

Display the global GVRP configuration.

**Syntax** `show config`

**Command Modes** CONFIGURATION-GVRP

**Supported Modes** Full-Switch

### Command History

#### Version

#### Description

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 or number information:
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 3/0        Disabled          No
Te 3/1        Disabled          No
Te 3/2        Enabled           No
Te 3/3        Disabled          No
Te 3/4        Disabled          No
Te 3/5        Disabled          No
Te 3/6        Disabled          No
```

Te 3/7	Disabled	No
Te 3/8	Disabled	No

**Related Commands** [show gvrp statistics](#) — displays the GVRP statistics.

## clear gvrp statistics

Clear GVRP statistics on an interface.

**Syntax** `clear gvrp statistics {interface interface | summary}`

**Parameters**

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

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

**summary** Enter the keyword `summary` to display just a summary of the GVRP statistics.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 1 - 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 tengig 1/0

Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
```

```
Failed Registrations: 0
Dell#
```

**Related Commands** [show gvrp](#) — displays the GVRP configuration.

## show vlan

Display the global VLAN configuration.

**Syntax** `show vlan`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell# show vlan
Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring
VLANs, P -
Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT
tagged
      NUM Status Description      Q Ports
*      1   Active
                               U Te 3/7
                               U Te 5/7-8

G     10   Active
                               G Po128(Te 5/10) (dynamically
learned vlan)
Dell
```

**Related Commands** [show gvrp statistics](#) — displays the GVRP statistics.



# Internet Group Management Protocol (IGMP)

The Dell Networking OS supports IGMP snooping version 2 and 3 on all Dell Networking systems.

## Topics:

- IGMP Commands
- IGMP Snooping Commands
- clear ip igmp groups
- debug ip igmp
- ip igmp access-group
- ip igmp group-join-limit
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-resp-time
- ip igmp snooping enable
- ip igmp snooping fast-leave
- ip igmp snooping flood
- ip igmp snooping last-member-query-interval
- ip igmp snooping mrouter
- ip igmp snooping querier
- ip igmp version
- show ip igmp groups
- show ip igmp interface
- show ip igmp snooping mrouter

## IGMP Commands

The Dell Networking OS supports the following IGMP commands:

- clear ip igmp groups
- debug ip igmp
- ip igmp group-join-limit
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-resp-time
- ip igmp snooping enable
- ip igmp snooping fast-leave
- ip igmp snooping flood
- ip igmp snooping last-member-query-interval
- ip igmp snooping mrouter
- ip igmp snooping querier
- ip igmp version
- show ip igmp groups
- show ip igmp interface
- show ip igmp snooping mrouter

## Important Points to Remember

- 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.
- IGMP snooping is enabled by default on the switch.
- A maximum of 2k groups and 4k virtual local area networks (VLAN) are supported.
- IGMP snooping is not supported on default VLAN interface.
- Flooding of unregistered multicast traffic is enabled by default.
- Queries are not accepted from the server side ports and are only accepted from the uplink LAG.
- Reports and Leaves are flooded by default to the uplink LAG irrespective of whether it is an mrouter port or not.

## 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).

## clear ip igmp groups

Clear entries from the group cache table.

**Syntax** `clear ip igmp groups [group-address | interface]`

**Parameters**

<b>group-address</b>	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
<b>interface</b>	(OPTIONAL) Enter the interface type and slot/port information: For a VLAN interface enter the keyword vlan followed by a number from 1 to 4094.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# debug ip igmp

Enable debugging of IGMP packets.

<b>Syntax</b>	<code>debug ip igmp [group address   interface]</code> To disable IGMP debugging, enter the <code>no ip igmp</code> command. To disable all debugging, enter the <code>undebug all</code> command.								
<b>Defaults</b>	Disabled								
<b>Parameters</b>	<b>group-address</b> (OPTIONAL) Enter the IP multicast group address in dotted decimal format. <b>interface</b> (OPTIONAL) Enter the interface type and slot/port information: For a VLAN interface enter the keyword <code>vlan</code> followed by a number from 1 to 4094.								
<b>Command Modes</b>	EXEC Privilege								
<b>Supported Modes</b>	All Modes								
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td><b>8.3.17.0</b></td><td>Supported on the M I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.								

# ip igmp access-group

To specify access control for packets, use this feature.

<b>Syntax</b>	<code>ip igmp access-group access-list</code> To remove the feature, use the <code>no ip igmp access-group access-list</code> command.						
<b>Parameters</b>	<b>access-list</b> Enter the name of the extended ACL (16 characters maximum).						
<b>Defaults</b>	Not configured						
<b>Command Modes</b>	INTERFACE ( <i>conf-if-interface-slot/port</i> )						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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 group-join-limit

To limit the number of IGMP groups that can be joined in a second, use this feature.

<b>Syntax</b>	<code>ip igmp group-join-limit number</code>
<b>Parameters</b>	<b>number</b> Enter the number of IGMP groups permitted to join in a second. The range is from 1 to 10000.

<b>Defaults</b>	none
<b>Command Modes</b>	CONFIGURATION ( <i>conf-if-interface-slot/port</i> )
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

**Syntax** `ip igmp querier-timeout seconds`  
To return to the default value, use the `no ip igmp querier-timeout` command.

**Parameters** *seconds* Enter the number of seconds the router must wait to become the new querier. The range is from 60 to 300. The default is **125 seconds**.

**Defaults** **125 seconds**

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## 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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

**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

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## 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

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**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 ip igmp snooping fast-leave` command.

**Defaults** Not configured.

**Command Modes** INTERFACE VLAN — (conf-if-vl-n)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information** Queriers normally send some queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a fast deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

## ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets. When flooding is disabled, unregistered multicast data traffic is forwarded to *only* multicast router ports in a VLAN. If there is no multicast router port in a VLAN, unregistered multicast data traffic is dropped.

**Syntax** `ip igmp snooping flood`  
To disable the flooding, use the `no ip igmp snooping flood` command.

**Parameters** Enabled

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## 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.

<b>Parameters</b>	<b><i>milliseconds</i></b>	Enter the interval in milliseconds. The range is from 100 to 65535. The default is <b>1000 milliseconds</b> .
<b>Defaults</b>	<b>1000 milliseconds</b>	
<b>Command Modes</b>	INTERFACE VLAN	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip igmp snooping mrouter interface <i>interface</i></code>	
	To delete a specific multicast router interface, use the <code>no igmp snooping mrouter interface <i>interface</i></code> command.	
<b>Parameters</b>	<b><i>interface</i></b> <b><i>interface</i></b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> </ul>
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	INTERFACE VLAN — (conf-if-vl- <i>n</i> )	
<b>Supported Modes</b>	Programmable-Mux (PMUX)	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>Usage Information</b>	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 <code>ip igmp snooping mrouter interface</code> 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.

<b>Syntax</b>	<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.	
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	INTERFACE VLAN — (conf-if-vl- <i>n</i> )	

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**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.

## ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

**Syntax** `ip igmp version {2 | 3}`

**Parameters**

<b>2</b>	Enter the number 2 to set the IGMP version number to IGMPv2.
<b>3</b>	Enter the number 3 to set the IGMP version number to IGMPv3.

**Defaults** 2 (that is, IGMPv2)

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## show ip igmp groups

View the IGMP groups.

**Syntax** `show ip igmp groups [group-address [detail] | detail | interface [group-address [detail]]]`

**Parameters**

<b>group-address</b>	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
<b>interface</b>	(OPTIONAL) Enter the interface type and slot/port information: For a VLAN interface enter the keyword <code>vlan</code> followed by a number from 1 to 4094.
<b>detail</b>	(OPTIONAL) Enter the keyword <code>detail</code> to display the IGMPv3 source information.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes



## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## Example

```
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
Member Ports: Po 2
225.0.0.2 Vlan 100 IGMPv2 00:00:05
00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.3 Vlan 100 IGMPv2 00:00:05
00:02:04 3.0.0.51
Member Ports: Po 2
225.0.0.4 Vlan 100 IGMPv2 00:00:05
00:02:04 3.0.0.51
Member Ports: Po 2
```

Field	Description
<b>Group Address</b>	Lists the multicast address for the IGMP group.
<b>Interface</b>	Lists the interface type, slot and port number.
<b>Mode</b>	Displays the IGMP version used.
<b>Uptime</b>	Displays the amount of time the group has been operational.
<b>Expires</b>	Displays the amount of time until the entry expires.
<b>Last Reporter</b>	Displays the IP address of the last host to be a member of the IGMP group.
<b>Member Ports</b>	Indicates the member ports of 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.

## show ip igmp interface

View information on the interfaces participating in IGMP.

**Syntax** `show ip igmp interface [interface]`

**Parameters**

<b>interface</b>	(OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface: <ul style="list-style-type: none"><li>For a Port Channel interface, enter the keyword port-channel followed by a number. Range: 1-128</li><li>For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.</li><li>For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.</li></ul>
------------------	---

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Example**

```
Dell#show ip igmp interface
Vlan 2 is up, line protocol is down
Inbound IGMP access group is not set
Interface IGMP group join rate limit is not set
IGMP snooping is enabled on interface
IGMP Snooping query interval is 60 seconds
IGMP Snooping querier timeout is 125 seconds
IGMP Snooping last member query response interval is 1000 ms
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
Vlan 3 is up, line protocol is down
Inbound IGMP access group is not set
Interface IGMP group join rate limit is not set
IGMP snooping is enabled on interface
IGMP Snooping query interval is 60 seconds
IGMP Snooping querier timeout is 125 seconds
IGMP Snooping last member query response interval is 1000 ms
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
--More--
```

## show ip igmp snooping mrouter

Displays multicast router interfaces.

**Syntax** `show ip igmp snooping mrouter [vlan number]`

**Parameters** **vlan number** Enter the keyword vlan followed by the vlan number. Range: 1 to 4094

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Example**

```
Dell#show ip igmp snooping mrouter vlan 2
Interface Router Ports
Vlan 2 Po 128
Dell#
```

**Related Commands**

[show ip igmp groups](#) — Use this IGMP command to view groups.

# Interfaces

This chapter defines the interface commands on the Aggregator switch.

## Topics:

- [Basic Interface Commands](#)
- [Port Channel Commands](#)
- [Time Domain Reflectometer \(TDR\) Commands](#)
- [UDP Broadcast](#)
- [Port Interface Commands](#)
- [Virtual LAN \(VLAN\) Commands](#)

## Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

### clear counters

Clear the counters used in the `show interfaces` commands for VLANs, and physical interfaces, or selected ones.

**Syntax** `clear counters interface`

**Defaults** Without a specific interface specified, the command clears all interface counters.

**Parameters** **interface** (OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface:

- For the management interface on the stack-unit, enter the keyword `managementethernet` followed by slot/port information. The slot and port range is 0.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keyword `port-channel` followed by a number. Range: 1-128

**NOTE:** This command also enables you to clear the port configurations corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to clear the port configurations corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM and added support to clear the interface configurations corresponding to a range of ports.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

```
Dell#clear counters
Clear counters on all interfaces [confirm]
```

## 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 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 information.

**Defaults** Without an interface specified, the command clears all interface dampening counters.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

On the switch, after you enter the `clear counters` command and verify the results with the `show interfaces` command, the line rate is not reset to 0.00%.

## Example

```
Dell#clear dampening tengigabitethernet 1/2
Clear dampening counters on tengig 1/2 [confirm] y
Dell#
```

### Related Commands

[show interfaces dampening](#) — displays interface dampening information.  
[dampening](#) — configures dampening on an interface.

## cx4-cable-length

Configure the length of the cable to be connected to the selected CX4 port.

**Syntax** `[no] cx4-cable-length {long | medium | short}`

**Parameters** **long | medium | short** Enter the keyword that matches the cable length to be used at the selected port:

- `short` = For 1-meter and 3-meter cable lengths.
- `medium` = For 5-meter cable length.
- `long` = For 10-meter and 15-meter cable lengths.

**Defaults** **medium**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

This command only works on ports that the system recognizes as CX4 ports. The figures below shows an attempt to configure an XFP port with the command after inserting a CX4 converter into the port.

For details about using XFP ports with CX4 cables, refer to your FN IOM switch hardware guide.

### Example (Unsuccessful)

```
Dell#show interfaces tengigabitethernet 0/26 | grep "XFP type"
Pluggable media present, XFP type is 10GBASE-CX4

Dell(conf-if-te-0/26)#cx4-cable-length short
% Error: Unsupported command.
Dell(conf-if-te-0/26)#cx4-cable-length medium
% Error: Unsupported command.
Dell(conf-if-te-0/26)#cx4-cable-length long
% Error: Unsupported command.
Dell(conf-if-te-0/26)#
```

### Example (Successful)

```
Dell#config
Dell(config)#interface tengigabitethernet 0/5
Dell(conf-if-0/5)#cx4-cable-length long
Dell(conf-if-0/5)#show config
!
interface TenGigabitEthernet 0/4
  no ip address
  cx4-cable-length long
  shutdown
Dell(conf-if-0/5)#exit
Dell(config)#
```

### Related Commands

[show config](#) – displays the configuration of the selected interface.

## dampening

Configure dampening on an interface.

### Syntax

```
dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]
```

To disable dampening, use the `no dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]` command.

### Parameters

<b><i>half-life</i></b>	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 <b>5 seconds</b> .
<b><i>reuse-threshold</i></b>	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 <b>750</b> .
<b><i>suppress-threshold</i></b>	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 <b>2500</b> .
<b><i>max-suppress-time</i></b>	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 <b>20 seconds</b> .

### Defaults

Disabled.

### Command Modes


INTERFACE (conf-if-)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** With each flap, the 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-3/2)#dampening 20 800 4500 120
Dell(conf-if-te-3/2)#
```

### Related Commands

[clear dampening](#) — clears the dampening counters on all the interfaces or just the specified interface.

[show interfaces dampening](#) — displays interface dampening information.

## description

Assign a descriptive text string to the interface.

**Syntax** `description desc_text`  
To delete a description, enter `no description` command.

**Parameters** *desc\_text* Enter a text string up to 240 characters long.

**Defaults** No description is defined.

**Command Modes** INTERFACE

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information**

- 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 default `vlan-id` command overwrites any previous text string configured as the description.
- The `show tdr` and default `vlan-id` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

### Related commands

[show interfaces description](#) — Displays the description field of interfaces.

## errdisable recovery cause

Enable automatic recovery of an interface from the Err-disabled state.

<b>Syntax</b>	<code>errdisable recovery cause {bpduguard   fefd   maclearnlimit   arp-inspection}</code>  To disable the automatic recovery, use the <code>no errdisable recovery cause {bpduguard   fefd   maclearnlimit   arp-inspection}</code> command.								
<b>Parameters</b>	<table><tr><td><b>bpduguard</b></td><td>Enter the keyword <code>bpduguard</code> to enable the timer to recover the interface from BPDU Guard error.</td></tr><tr><td><b>fefd</b></td><td>Enter the keyword <code>fefd</code> to enable the timer to recover the interface from FEFD error.</td></tr><tr><td><b>maclearnlimit</b></td><td>Enter the keyword <code>maclearnlimit</code> to enable the timer to recover the interface from MAC learning limit error.</td></tr><tr><td><b>arp-inspection</b></td><td>Enter the keyword <code>arp-inspection</code> to enable the timer to recover the interface from an arp-inspection error.</td></tr></table>	<b>bpduguard</b>	Enter the keyword <code>bpduguard</code> to enable the timer to recover the interface from BPDU Guard error.	<b>fefd</b>	Enter the keyword <code>fefd</code> to enable the timer to recover the interface from FEFD error.	<b>maclearnlimit</b>	Enter the keyword <code>maclearnlimit</code> to enable the timer to recover the interface from MAC learning limit error.	<b>arp-inspection</b>	Enter the keyword <code>arp-inspection</code> to enable the timer to recover the interface from an arp-inspection error.
<b>bpduguard</b>	Enter the keyword <code>bpduguard</code> to enable the timer to recover the interface from BPDU Guard error.								
<b>fefd</b>	Enter the keyword <code>fefd</code> to enable the timer to recover the interface from FEFD error.								
<b>maclearnlimit</b>	Enter the keyword <code>maclearnlimit</code> to enable the timer to recover the interface from MAC learning limit error.								
<b>arp-inspection</b>	Enter the keyword <code>arp-inspection</code> to enable the timer to recover the interface from an arp-inspection error.								
<b>Defaults</b>	Disabled								
<b>Command Modes</b>	CONFIGURATION								
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .								
	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.14(1.0)</b></td><td>Introduced <code>arp-inspection</code> option.</td></tr><tr><td><b>9.14(0.0)</b></td><td>Introduced on the platforms S4048-ON, S6100-ON, Z9100-ON, S4048T-ON, S3048-ON, S6000, S6010-ON, S5048F-ON, FN-IOM and MXL.</td></tr><tr><td><b>9.13(0.2P2)</b></td><td>Introduced on the S3100.</td></tr></tbody></table>	Version	Description	<b>9.14(1.0)</b>	Introduced <code>arp-inspection</code> option.	<b>9.14(0.0)</b>	Introduced on the platforms S4048-ON, S6100-ON, Z9100-ON, S4048T-ON, S3048-ON, S6000, S6010-ON, S5048F-ON, FN-IOM and MXL.	<b>9.13(0.2P2)</b>	Introduced on the S3100.
Version	Description								
<b>9.14(1.0)</b>	Introduced <code>arp-inspection</code> option.								
<b>9.14(0.0)</b>	Introduced on the platforms S4048-ON, S6100-ON, Z9100-ON, S4048T-ON, S3048-ON, S6000, S6010-ON, S5048F-ON, FN-IOM and MXL.								
<b>9.13(0.2P2)</b>	Introduced on the S3100.								
<b>Usage Information</b>	This command has to be configured before the interface moves to Err-disabled state. If not, the recovery action is not performed.								
<b>Related Commands</b>	<a href="#">errdisable recovery interval</a> — Configure recovery timer interval for an interface.								

## errdisable recovery interval

Configure recovery time interval to move an interface from the Err-disabled state.

<b>Syntax</b>	<code>errdisable recovery interval seconds</code>  To remove the configured recovery time interval, use the <code>no errdisable recovery interval seconds</code> command.		
<b>Parameters</b>	<table><tr><td><b>interval seconds</b></td><td>Enter the keyword <code>interval</code> and the number of seconds to recover the interface from Err-disabled state. The range is from 30 to 86,400 seconds. The default is 300 seconds.</td></tr></table>	<b>interval seconds</b>	Enter the keyword <code>interval</code> and the number of seconds to recover the interface from Err-disabled state. The range is from 30 to 86,400 seconds. The default is 300 seconds.
<b>interval seconds</b>	Enter the keyword <code>interval</code> and the number of seconds to recover the interface from Err-disabled state. The range is from 30 to 86,400 seconds. The default is 300 seconds.		
<b>Defaults</b>	300 seconds.		
<b>Command Modes</b>	CONFIGURATION		
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .		

Version	Description
9.14(0.0)	Introduced on the platforms S4048-ON, S6100-ON, Z9100-ON, S4048T-ON, S3048-ON, S6000, S6010-ON, S5048F-ON, FN-IOM, and MXL.
9.13(0.2P2)	Introduced on the S3100.

### Usage Information

Whenever the Err-disable recovery timer is reconfigured, it will get effective only after the current timer expires. Following message is displayed after each Err-disable recovery timer configuration:

```
DellEMC(conf)# errdisable recovery interval 30
New timer interval will be effective from the next timer instance only.
```

### Related Commands

[errdisable recovery cause](#) — Enable automatic recovery of an interface from the error disabled state.

## flowcontrol

Controls how the system responds to and generates 802.3x pause frames on 10G and 40Gig stack units.

**Syntax** `flowcontrol rx {off | on} tx {off | on} pause-threshold value [monitor session-ID]`

### Parameters

<b>rx on</b>	Enter the keywords <code>rx on</code> to process the received flow control frames on this port. This is the default value for the receive side.
<b>rx off</b>	Enter the keywords <code>rx off</code> to ignore the received flow control frames on this port.
<b>tx on</b>	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. This is the default value on the send side.
<b>tx off</b>	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.
<b>pause-threshold</b>	Enter the buffer threshold limit for generating PAUSE frames.
<b>monitor</b>	Enter the keyword <code>monitor</code> then the session-ID to enable mirror flow control frames on the interface. The range is from 0 to 65535.

### Defaults

- `rx off`
- `tx off`

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

### Command History

Version	Description
9.11(0.0)	Added support for monitor session.
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

The pause:



- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the switch. The discard threshold should be larger than the *buffer threshold* so that the buffer holds at least hold at least three packets.

### Important Points to Remember

- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Asymmetric flow control (`rx on tx off`, or `rx off tx on`) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

```
Can't configure Asymmetric flowcontrol when speed <1G, config ignored
```

- The only configuration applicable to half duplex ports is `rx off tx off`. The following error is returned:

```
Cannot configure Asymmetric flowcontrol when speed <1G, config ignored>
```

- You cannot configure half duplex when the flow control configuration is on (default is `rx on tx on`). The following error is returned: `Cannot configure half duplex when flowcontrol is on, config ignored`

**i** **NOTE:** The flow control must be off (`rx off tx off`) before configuring the half duplex.

### Example (partial)

```
Dell(conf-if-tengig-0/1)#show config
!
interface TenGigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol monitor session 5 rx off tx on
no shutdown
...
```

**Example (Values)** This Example shows how the 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         off         off           on
off         off         on           off
off         off         on           on

off         on         off           off
off         on         off           on
off         on         on           off
off         on         on           on

on         off         off           off
on         off         off           on
on         off         on           off
on         off         on           on

on         on         off           off
on         on         off           on
on         on         on           off
on         on         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).

## interface

Configure a physical interface on the switch.

**Syntax** `interface interface`

**Parameters** *interface* Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information**

You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are in Layer 3 mode. To place an interface in mode, ensure that the interface's configuration does not contain an IP address and enter the `Port Channel Commands` command. By default, the interface is shut down when the `portmode hybrid` and `switchport` are enabled.

The tunnel interface operates as an ECMP (equal cost multipath) 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(conf)#interface tengig 0/1
Dell(conf-if-te-0/1)#exit#

```

**Related Commands**

[interface port-channel](#) — configures a port channel.

[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** ***number*** Enter a number as the interface number. The range is from 0 to 16383.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf)#interface loopback 1655
Dell(conf-if-lo-1655)#
```

**Related Commands**

- [interface](#) — configures a physical interface.
- [interface null](#) — configures a Null interface.
- [interface port-channel](#) — configures a port channel.
- [interface vlan](#) — configures a VLAN.

## interface ManagementEthernet

Configure the Management port on the system.

**Syntax** `interface ManagementEthernet slot/port`

**Parameters** ***slot/port*** Enter the keyword `ManagementEthernet`, then the slot number (0) and port number zero (0).

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4.(0.0)</b>	Supported on the FN I/O Aggregator and M I/O Aggregator.

**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.

### Example

```
Dell(conf)#interface managementethernet 0/0
Dell(conf-if-ma-0/0)#
```

## 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachable`.

**Example**

```
Dell(conf)#interface null 0
Dell(conf-if-nu-0)#
```

**Related Commands**

[interface](#) — configures a physical interface.

[interface loopback](#) — configures a Loopback interface.

[interface port-channel](#) — configures a port channel.

[interface vlan](#) — configures a VLAN.

`ip unreachable` — 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, interface,...`

To delete a description, enter `no description` command.

**Parameters**

**interface, interface,...** Enter the keyword `interface range` and one of the interfaces — slot/port, port-channel or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces.

Slot/Port information must contain a space before and after the dash. For example, `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is not valid.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

## Command History

Version	Description
9.14(0.0)	Updated the error message when no ports are configured within the specified interface range.
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

## 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 things to remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The interface range prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis ( ... ).
- 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-If no ports are configured within the specified interface range

```
Dell(conf)#interface range tengig 0/1 - 2 , tengig 0/4 , tengig 0/7
, fa 0/0
% Error: No port is configured in interface range
```

### Example-Bulk Configuration Warning Message

```
Dell(conf)#interface range tengig 0/1 - 2 , tengig 0/4 , tengig 0/7
, fa 0/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

### Example-Interface Range prompt with Multiple Ports

```
Dell(conf)#interface range tengig 0/1 - 2 , tengig 0/3 - 5
Dell(conf-if-range-te-0/1-5)#
```

### Example-Interface Range prompt Overlapping Port Ranges

```
Dell(conf)#interface range tengig 0/1 - 2 , tengig 0/1 - 5
Dell(conf-if-range-te-0/1-5)#
```

Only VLAN and port-channel interfaces created using the `interface vlan` and `vlan tagged` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

**i** **NOTE:** If a range has VLAN, physical, and port-channel interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

### Example-Single Range Bulk Configuration

```
Dell(conf)# interface range tengigabitethernet 0/1 - 5
Dell(conf-if-range-te-0/1-5)# no shutdown
Dell(conf-if-range-te-0/1-5)#
```

### Example-Multiple Range Bulk Configuration with VLAN and port channel

The following example shows how to use commas to add VLAN and port-channel interfaces to the range.

```
Dell(conf-if)# interface range tengigabitethernet 0/1 - 5, vlan 2 - 10,
port-channel 1 - 25
```

```
Dell (conf-if-range-te-0/1-5,vl-2-10,po-1-25)# no shutdown
Dell (conf-if-range-te-0/1-5,vl-2-10,po-1-25)#
```

### Related commands

[show config \(from INTERFACE RANGE mode\)](#) — Shows the bulk configuration interfaces.  
[show interfaces status](#) — Displays a summary of interface information.

## interface range macro (define)

Defines a macro for an interface range and then saves the macro in the running configuration.

**Syntax** `define interface range macro name interface , interface , ...`

### Parameters

- |   |  |
|---|--|
| <b><i>name</i></b>                                | Enter up to 16 characters for the macro name.  |
| <b><i>interface</i>,<br/><i>interface</i>,...</b> | Enter the keywords <code>interface range</code> and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces.<br><br>Slot/Port information must contain a space before and after the dash. For example, <code>interface range tengigabitethernet 0/1 - 5</code> is valid; <code>interface range tengigabitethernet 0/1-5</code> is NOT valid. <ul style="list-style-type: none"><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul> |

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 tengigabitethernet0/0-3,
tengigabitethernet 5/0-7

Dell# show running-config | grep define
define interface-range test tengigabitethernet0/0-3,
tengigabitethernet5/0-7,
Dell(config)#interface range macro test
Dell (config-if-range-te-0/0-3,te-5/0-7) #
```

### 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** *name* Enter the name of an existing macro.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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-0/0-3,te-5/0-8)#
```

**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. Configure the default VLAN to enable Static or DHCP IP configuration. You can configure up to 4094 VLANs.

**Syntax** `interface vlan vlan-id`

To delete a VLAN, use the `no interface vlan vlan-id` command.

**Parameters** *vlan-id* Enter 1 for the default VLAN. Enter a number as the VLAN identifier. The range is from 1 to 4096.

**Defaults** Not configured, except for the default VLAN, which is configured as VLAN 1.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** For more information about VLANs and the commands to configure them, refer to [Virtual LAN \(VLAN\) Commands](#).

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC/IP ACLs are not supported.

## Examples

```
Dell(conf)#int vlan 1
Dell(conf-if-vl-1)#
```

```
Dell(conf)#int vlan 3
Dell(conf-if-vl-3)#
```

## Related commands

[show vlan](#) — Displays the current VLAN configuration on the switch.

[vlan tagged](#) — Adds a Layer 2 interface to a VLAN as a tagged interface.

[vlan 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** `intf-type cr4 autoneg`

If you configure `intf-type cr4 autoneg`, use the `no intf-type cr4 autoneg` command to set the interface type as cr4 with autonegotiation disabled.

**Defaults** Not configured

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

### Usage Information

If you configure `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.

### Related Commands

[interface](#) — configures a physical 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** `keepalive [seconds]`

To stop sending keepalive packets, use the `no keepalive` command.

**Parameters** **seconds** (OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is **10 seconds**.

**Defaults** Enabled.

**Command Modes** INTERFACE

**Supported Modes** All Modes

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.



Version	Description
9.2(0.0)	Supported on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

## load-balance

By default, 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:

 **NOTE:** The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

`dest-ip` — Uses destination IP address and destination port fields to hash.

`source-ip` — Uses source IP address and source port fields to hash.

#### mac {dest-mac | source-dest-mac | source-mac}

Enter the keywords to distribute MAC traffic based on the following criteria:

`dest-mac` — Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash.

`source-dest-mac` — Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash.

`source-mac` — Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash.

#### tcp-udp enable

Enter the keywords to distribute traffic based on the following:

`enable` — Takes the TCP/UDP source and destination ports into consideration when doing hash computations. This option is enabled by default.

`ingress-port enable`—Enter the keywords to distribute traffic based on the following:

`enable` — Takes the source port into consideration when doing hash computations. This option is disabled by default.

### Defaults

IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

### Command Modes

CONFIGURATION

### Supported Modes

Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 higig links.

### Syntax

```
[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]}
```

### 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-port | L4-dest-port ]**

To use IPv4 key fields in hash computation, enter the keyword ip-selection then one of the parameters. To use IPv6 key fields in hash computation, enter the keyword ipv6-selection then one of the parameters.

- source-ip — Use IPv4 src-ip field in hash calculation.
- source-ipv6 — Use IPv6 src-ip 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-ip — Use IPv4 dest-ip field in hash calculation
- dest-ipv6 — Use IPv6 dest-ip 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.
- 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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** `monitor interface [interface]`  
 To disable monitoring and return to the CLI prompt, press the `q` key.

**Parameters** *interface* (OPTIONAL) Enter the following keywords and slot/port or number information:

- For the management port, enter the keyword `managementethernet` then the slot (0 or 1) and the port (0).
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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
<b>sysstest-3</b>	Displays the host name assigned to the system.
<b>monitor time</b>	Displays the amount of time since the <code>monitor interface</code> command was entered.
<b>time</b>	Displays the amount of time the chassis is up (since last reboot).
<b>m</b>	Change the view from a single interface to all interfaces on the line card or visa-versa.
<b>c</b>	Refresh the view.
<b>b</b>	Change the counters displayed from Packets on the interface to Bytes.
<b>r</b>	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
<b>l</b>	Change the view to the next interface on the line card, or if in line card mode, the next line card in the chassis.
<b>a</b>	Change the view to the previous interface on the line card, or if in line card mode, the previous line card in the chassis.
<b>T</b>	Increase the screen refresh rate.
<b>t</b>	Decrease the screen refresh rate.
<b>q</b>	Return to the CLI prompt.

## Example (Single Interface)

```
systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time: 03:26:26

Interface: Te 0/3, 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
```

## 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. The default is **1554**.

**Defaults** **1554**

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

- The IP MTU is adjusted automatically when you configure the Layer 2 MTU with the `mtu` command.

When you enter the `no mtu` command, The 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, enter `no negotiation auto` command.

**Defaults** Enabled.

**Command Modes** INTERFACE

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information** The `no negotiation auto` command is only available if you first manually set the speed of a port to **10Mbits** or **100Mbits**.

#### Example (Configured)

```
Dell#show interfaces configured
TenGigabitEthernet 0/1 is up, line protocol is up
Hardware is DellEth, address is 00:1e:c9:de:04:9c
  Current address is 00:1e:c9:de:04:9c
Server Port AdminState is N/A
Pluggable media not present
Interface index is 33886978
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :001ec9de049c
```

```

MTU 12000 bytes, IP MTU 11982 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:56:48
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.

#### Related Commands

[speed \(for 1000/10000 interfaces\)](#) — sets the link speed to 10, 100, 1000 or auto-negotiate the speed.

## 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)`

**Supported Modes** `Full-Switch`

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

**i** **NOTE:** Remove all other configurations on the port before you can remove the hybrid configuration from the port.

## Example

```
Dell(conf)#interface tengig 0/2
Dell(conf-if-te-0/2)#no shut
Dell(conf-if-te-0/2)#portmode hybrid
Dell(conf-if-te-0/2)#sw
Dell(conf-if-te-0/2)#int vlan 10
Dell(conf-if-vl-10)#tag tengig 0/2
Dell(conf-if-vl-10)#int vlan 20
Dell(conf-if-vl-20)#untag tengig 0/2
Dell(conf-if-vl-20)#
```

## Example (tagged hybrid)

```
Dell(conf)#interface tengig 0/2
Dell(conf-if-te-0/2)#no shut
Dell(conf-if-te-0/2)#portmode hybrid
Dell(conf-if-te-0/2)#sw
Dell(conf-if-te-0/2)#int vlan 10
Dell(conf-if-vl-10)#int tengig 0/2
Dell(conf-if-vl-20)# untag tengig 0/2

Dell (conf-if-vl-20)#

Dell(conf)#do show interfaces switchport tengigabitethernet 3/2

Codes: U - Untagged, T - Tagged
       x - Dot1x untagged, X - Dot1x tagged
       G - GVRP tagged, M - Trunk, H - VSN tagged
       i - Internal untagged, I - Internal tagged, v - VLT untagged,
       V - VLT tagged

Name: TenGigabitEthernet 3/2

802.1QTagged: Hybrid
Vlan membership:
Q   Vlans
U   20
T   10

Native VlanId: 20.

Dell(conf)#
```

## Example (unconfigure the hybrid port)

```
Dell(conf-if-vl-20)#interface vlan 10
Dell(conf-if-vl-10)#no untagged tengig 0/2
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#no tagged tengig 0/2
Dell(conf-if-vl-20)#interface tengig 0/2
Dell(conf-if-te-0/2)#no portmode hybrid
Dell(conf-if-vl-20)#
```

**Related Commands** [show interfaces switchport](#) — displays the configuration of switchport (Layer 2) interfaces on the switch.  
[vlan-stack trunk](#)— specifies an interface as a trunk port to the Stackable VLAN network.

## rate-interval

Configure the traffic sampling interval on the selected interface.

**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.

**i** **NOTE:** For 0 to 5 seconds, polling occurs every 5 seconds. For 6 to 10 seconds, polling occurs every 10 seconds. For any other value, polling occurs every 15 seconds.

**Defaults** **299 seconds**

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.

**Related Commands** [show interfaces](#) — displays information on physical and virtual interfaces.

## rate-interval (Configuration Mode)

Configure the traffic sampling interval for all physical and logical port-channel interfaces globally. The support to configure rate-interval globally enables you to modify the default interval rate for all physical and logical interfaces at one time.

**Syntax** `rate-interval seconds`

Use the `no rate-interval` command to remove the sampling interval configuration.

**Parameters** **seconds** Enter the number of seconds for which to collect traffic data. The range is from 5 to 299 seconds.

**i** **NOTE:** Because polling occurs every 15 seconds, the number of seconds designated here round to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated, it rounds to 30; 45 to 59 seconds rounds to 45. If you configure this value to be less than 5, then the entire buffer is cleared; the `show int stats` command shows the rate information to be 0 as the polling interval is less than 5.

**Defaults** **299 seconds**

**Command Modes** CONFIGURATION

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



Version	Description
9.11.0.0	Introduced on all Dell Networking OS platforms.

#### Usage Information

The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.

When rate-interval is not configured in the global configuration mode or interface mode, the default value of 299 seconds is applied.

When rate-interval is configured only in the global configuration mode and not in the interface mode, the global rate-interval value is applied at the interface level also.

When rate-interval is configured at the interface level and not in the global configuration mode, the interface level rate-interval value is applied for an interface.

When rate interval is configured in both global configuration mode as well as interface mode, then the rate-interval value configured at interface level is applied as it takes precedence over the global value.

## remote-fault-signaling rx

Brings the interface up or down when a Remote Fault Indication (RFI) error is detected.

**Syntax** `remote-fault-signaling rx {on | off}`

**Parameters**

- on** Brings the interface up when an RFI error is detected.
- off** Brings the interface down when an RFI error is detected.

**Defaults** ON.

**Command Modes** INTERFACE CONFIGURATION

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL switch.

#### Usage Information

By default, the switch processes the RFI errors transmitted by remote peers and brings down the interface when an RFI error is detected.

#### Example

```
Dell(conf-if-te-1/3)#remote-fault-signaling rx ?
on Enable
off Disable
```

## show config

Display the interface configuration.

**Syntax** `show config`

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell(conf-if)#show conf
!
interface TenGigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
Dell(conf-if)#
```

## show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (group).

**Syntax** `show config`

**Command Modes** CONFIGURATION INTERFACE (conf-if-range)

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

## show interfaces

Displays information on a specific physical interface or virtual interface.

**Syntax** `show interfaces interface`

**Parameters** ***interface*** Enter one of the following keywords and slot/port or number information:

- For the management interface on the stack-unit, enter the keyword `managementethernet` followed by slot/port information. The slot and port range is 0.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` 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 keyword `port-channel` followed by a number. The range is from 1 to 128.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information** Use this `show interfaces` command for details on a specific interface. Use the `show interfaces stack-unit` command for details on all interfaces on the designated stack unit.

On the I/O Aggregator, the show interface output displays incorrect rate information details over time for link monitoring when the rate-interval is configured for 5 seconds. Dell Networking recommends using higher rate-intervals such as 15 to 299 seconds to minimize the errors seen.

**NOTE:** In the CLI output, the power value will be rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an snmp query will return 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 will be no change in the line-rate.

**User Information** The following describes the `show interfaces` command shown in the 10G example below.

Line	Description
<b>TenGigabitEthernet 0/0...</b>	Displays the interface's type, slot/port, and administrative and line protocol status.
<b>Hardware is...</b>	Displays the interface hardware information and its assigned MAC address.
<b>Interface index...</b>	Displays the interface index number used by SNMP to identify the interface.
<b>Internet address...</b>	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
<b>MTU 1554...</b>	Displays link and IP MTU information. If the chassis is in Jumbo mode, this number can range from 576 to 12000.
<b>LineSpeed</b>	Displays the interface's line speed.
<b>ARP type:...</b>	Displays the ARP type and the ARP timeout value for the interface.
<b>Last clearing...</b>	Displays the time when the <code>show interfaces</code> counters were cleared.
<b>Queuing strategy...</b>	States the packet queuing strategy. FIFO means first in first out.
<b>Input Statistics:</b>	Displays all the input statistics including: <ul style="list-style-type: none"><li>• Number of packets and bytes into the interface</li><li>• Number of packets with IP headers and VLAN tagged headers.<ul style="list-style-type: none"><li><b>NOTE:</b> The sum of the number of packets may not be as expected since a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.</li></ul></li><li>• Packet size and the number of those packets inbound to the interface</li><li>• Number of symbol errors, runts, giants, and throttles packets:<ul style="list-style-type: none"><li>◦ symbol errors = number packets containing bad data. That is, the port MAC detected a physical coding error in the packet.</li><li>◦ runts = number of packets that are less than 64B</li><li>◦ giants = packets that are greater than the MTU size</li><li>◦ throttles = packets containing PAUSE frames</li></ul></li><li>• Number of CRC, IP Checksum, overrun, and discarded packets:<ul style="list-style-type: none"><li>◦ CRC = packets with CRC/FCS errors</li><li>◦ IP Checksum = packets with IP Checksum errors</li><li>◦ overrun = number of packets discarded due to FIFO overrun conditions</li><li>◦ discarded = the sum of runts, giants, CRC, IP Checksum, and overrun packets discarded without any processing</li></ul></li></ul>
<b>Output Statistics:</b>	Displays output statistics sent out of the interface including: <ul style="list-style-type: none"><li>• Number of packets, bytes, and underruns out of the interface<ul style="list-style-type: none"><li>◦ packets = total number of packets</li><li>◦ bytes = total number of bytes</li><li>◦ underruns = number of packets with FIFO underrun conditions</li></ul></li><li>• Number of Multicast, Broadcast, and Unicast packets:<ul style="list-style-type: none"><li>◦ Multicasts = number of MAC multicast packets</li><li>◦ Broadcasts = number of MAC broadcast packets</li><li>◦ Unicasts = number of MAC unicast packets</li></ul></li><li>• Number of throttles and discards packets:<ul style="list-style-type: none"><li>◦ throttles = packets containing PAUSE frames</li><li>◦ discarded = number of packets discarded without any processing</li></ul></li></ul>

Line	Description
<b>Rate information...</b>	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.
<b>Time since...</b>	Elapsed time since the last interface status change (hh:mm:ss format).

### Usage Information

The interface counter “over 1023-byte pkts” does not increment for packets in the range  $9216 > x < 1023$ .  
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.

### Example (ManagementEthernet)

```
Dell#show interface managementethernet ?
0/0 Management Ethernet interface number
Dell#show interface managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
Current address is 00:1e:c9:f1:00:05
Pluggable media not present
Interface index is 235159752
Internet address is 10.11.209.87/16
Mode of IP Address Assignment : MANUAL
DHCP Client-ID: mgmt001ec9f10005
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 100 Mbit, Mode full duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 5d4h57m
Queueing strategy: fifo
Input 3448753 packets, 950008323 bytes, 3442163 multicast
Received 0 errors, 0 discarded
Output 4627 packets, 814226 bytes, 0 multicast
Output 0 errors, 0 invalid protocol
```

### Related Commands

- [show interfaces configured](#) — Displays any interface with a non-default configuration.
- [show interfaces port-channel](#) — Displays information on all interfaces on a specific stack unit.
- [show interfaces switchport](#) — Displays Layer 2 information about the interfaces.
- [show inventory](#) — Displays the I/O Aggregator type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.
- [show ip interface](#) — Displays Layer 3 information about the interfaces.
- [show memory](#) — Displays the stack unit(s) status.
- [show interfaces status](#) — Displays all interfaces configured using the interface range command.

## show interfaces configured

Displays any interface with a non-default configuration.

**Syntax** `show interfaces configured`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example (ManagementEthernet)

# show interfaces dampening

Display interface dampening information.

**Syntax** `show interfaces dampening [[interface] [summary] [detail]]`

### Parameters

#### ***interface***

(Optional) Enter one of the following keywords and slot/port or number information:

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

**NOTE:** This command also enables you to view information corresponding to a range of ports. However, for Open Networking (ON) platforms the notation for specifying port range in the command is different from how you specify in non-ON platforms.

- For non-ON platforms, you can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.
- For ON platforms, you can specify multiple ports as `slot/port/[subport] - slot/port/[subport]`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1/1 - 1/4/1`.

#### **summary**

(OPTIONAL) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.

#### **detail**

(OPTIONAL) Enter the keyword `detail` to display detailed interface dampening data.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

### Command History

#### **Version**

#### **Description**

**9.9(0.0)**

Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show interfaces dampening
Interface Supp   Flaps Penalty Half-Life Reuse Suppress Max-Sup
State
Te 3/2   Up     0     0      20      800   4500   120
Te 3/8   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 description

Display the descriptions configured on the interface.

**Syntax** `show interfaces [interface] description`

**Parameters** *interface*

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

- For the management interface on the stack unit enter the keyword `ManagementEthernet` followed by the slot/port information. The slot range is 0-0 and the port range is 0.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For VLAN interfaces, enter the keyword `vlan` followed by a number from 1 to 4094.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following describes the `show interfaces description` command shown in the Example below.

Field	Description
<b>Interface</b>	Displays the type of interface and associated slot and port number.
<b>OK?</b>	Indicates if the hardware is functioning properly.
<b>Status</b>	States whether the interface is enabled (up) or disabled (administratively down).
<b>Protocol</b>	States whether IP is enabled (up) or disabled (down) on the interface.
<b>Description</b>	Displays the description (if any) manually configured for the interface.

### Example

```
Dell#show interface description
Interface          OK   Status      Protocol   Description
TenGigabitEthernet 0/1  NO  admin down  down
TenGigabitEthernet 0/2  NO  admin up    down
TenGigabitEthernet 0/3  NO  admin up    down
TenGigabitEthernet 0/4  NO  admin up    down
TenGigabitEthernet 0/5  NO  admin up    down
TenGigabitEthernet 0/6  NO  admin up    down
TenGigabitEthernet 0/7  NO  up down
TenGigabitEthernet 0/8  YES  up up
```

## show interfaces stack-unit

Display information on all interfaces on a specific Aggregator stack member.

- Syntax** `show interfaces stack-unit unit-number`
- Parameters** *unit-number* Enter the stack member number (0 to 5).
- Command Modes**
- EXEC
  - EXEC Privilege
- Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
Dell#show interfaces stack-unit 0
TenGigabitEthernet 0/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:1e:c9:f1:00:05
Current address is 00:1e:c9:f1:00:05
Server Port AdminState is Down
Pluggable media not present
Interface index is 34148609
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :tenG130001ec9f10005
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 5d5h24m
Queueing strategy: fifo
Input Statistics:
0 packets, 0 bytes
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts
0 runts, 0 giants, 0 throttles
0 CRC, 0 overrun, 0 discarded
Output Statistics:
0 packets, 0 bytes, 0 underruns
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 throttles, 0 discarded, 0 collisions
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: 5d5h23m
!-----output truncated -----!
```

**Related Commands** [show diag](#) — Displays data plane and management plane input/output statistics.

## show interfaces status

Displays a summary of interface information or specify a stack unit and interface to display status information for that specific interface only.

**Syntax** `show interfaces [interface | stack-unit unit-number] status`

## Parameters

- interface*** (OPTIONAL) Enter one of the following keywords and slot/port or number information:
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- unit-number*** Enter the stack unit's ID number. The range is from 0 to 5.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- You can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

## Defaults

none

## Command Modes

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## Example

```
Dell#sh interfaces status
Port          Description      Status Speed      Duplex  Vlan
Te 2/1        Te 2/1          Down   Auto       Auto    --
Te 2/2        Te 2/2          Down   Auto       Auto    --
Te 2/3        Te 2/3          Down   Auto       Auto    --
Te 2/4        Te 2/4          Down   Auto       Auto    --
Te 2/5        Te 2/5          Down   Auto       Auto    --
Te 2/6        Te 2/6          Down   Auto       Auto    --
Te 2/7        Te 2/7          Down   Auto       Auto    --
Te 2/8        Te 2/8          Down   Auto       Auto    --
Te 2/9        Te 2/9          Up     10000 Mbit Full 1001
Te 2/10       Te 2/10         Down   Auto       Auto    --
Te 2/11       Te 2/11         Up     10000 Mbit Full 1001
Te 2/12       Te 2/12         Down   Auto       Auto    --
Dell#
```

# 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

```
show interfaces switchport [interface | stack-unit unit-id ]
```

## 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` followed by the slot/port information.
  - Enter the keyword `backup` to view the backup interface for this interface.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- For physical interfaces, you can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to



all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.

- For port-channel interfaces, you can specify multiple ports as `port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces port-channel 1 - 4`.

**stack-unit *unit-id*** (OPTIONAL) Enter the keywords `stack-unit` followed by the stack member number. The range is from 0 to 5.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information**

The following describes the `show interfaces switchport` command for the following example.

Items	Description
<b>Name</b>	Displays the interface's type, slot, and port number.
<b>802.1QTagged</b>	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid"), which supports both untagged and tagged VLANs by port 13/0.
<b>Vlan membership</b>	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#sh interfaces switchport

Codes:  U - Untagged, T - Tagged
        x - Dot1x untagged, X - Dot1x tagged
        G - GVRP tagged, M - Trunk, H - VSN tagged
        i - Internal untagged, I - Internal tagged, v - VLT untagged, V
        - VLT tagged

Name: TenGigabitEthernet 2/9
802.1QTagged: True
Vlan membership:
Q      Vlans
T      1001

Name: TenGigabitEthernet 2/11
802.1QTagged: True
Vlan membership:
Q      Vlans
T      1001

Dell#
```

**Related Commands**

[show ip interface](#) — displays Layer 3 information about the interfaces.

# 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 transceiver`

**Parameters** **tengigabitethernet** For a 10G interface, enter the keyword `tengigabitethernet` then the slot/port information.

**NOTE:** This command also enables you to view information corresponding to a range of ports. However, for Open Networking (ON) platforms the notation for specifying port range in the command is different from how you specify in non-ON platforms.

- For non-ON platforms, you can specify multiple ports as `slot/port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1 - 4`.
- For ON platforms, you can specify multiple ports as `slot/port/[subport] - slot/port/[subport]`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces interface-type 1/1/1 - 1/4/1`.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show interfaces transceiver` command shown in the following example.

Line	Description
<b>Rx Power measurement type</b>	Output depends on the vendor, typically either "Average" or "OMA" (Receiver optical modulation amplitude).
<b>Temp High Alarm threshold</b>	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
<b>Voltage High Alarm threshold</b>	Displays the interface index number used by SNMP to identify the interface.
<b>Bias High Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>TX Power High Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>RX Power High Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Temp Low Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Voltage Low Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.

<b>Line</b>	<b>Description</b>
<b>Bias Low Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>TX Power Low Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>RX Power Low Alarm threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Temp High Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Voltage High Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Bias High Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>TX Power High Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>RX Power High Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Temp Low Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Voltage Low Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Bias Low Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>TX Power Low Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Power Low Warning threshold</b>	Factory-defined setting. Value can differ between SFP and SFP+.
<b>Temperature</b>	Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.
<b>Voltage</b>	Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/warning flag is set to true.
<b>Tx Bias Current</b>	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.
<b>Tx Power</b>	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.
<b>Rx Power</b>	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.

<b>Line</b>	<b>Description</b>
<b>Data Ready state Bar</b>	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.
<b>Rx LOS state</b>	This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.
<b>Tx Fault state</b>	This is the digital state of the Tx Fault output pin.
<b>Rate Select state</b>	This is the digital state of the SFP rate_select input pin.
<b>RS state</b>	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
<b>Tx Disable state</b>	If the admin status of the port is down then this flag is set to true.
<b>Temperature High Alarm Flag</b>	This can be either true or false, depending on the Current voltage value displayed above.
<b>Voltage High Alarm Flag</b>	This can be either true or false, depending on the Current Temperature value displayed above.
<b>Tx Bias High Alarm Flag</b>	This can be either true or false, depending on the present Tx bias current value displayed above.
<b>Tx Power High Alarm Flag</b>	This can be either true or false, depending on the Current Tx bias power value displayed above.
<b>Rx Power High Alarm Flag</b>	This can be either true or false, depending on the Current Rx power value displayed above.
<b>Temperature Low Alarm Flag</b>	This can be either true or false, depending on the Current Temperature value displayed above.
<b>Voltage Low Alarm Flag</b>	This can be either true or false, depending on the Current voltage value displayed above.
<b>Tx Bias Low Alarm Flag</b>	This can be either true or false, depending on the Tx bias current value displayed above.
<b>Tx Power Low Alarm Flag</b>	This can be either true or false, depending on the Current Tx power value displayed above.
<b>Rx Power Low Alarm Flag</b>	This can be either true or false, depending on the Current Rx power value displayed above.
<b>Temperature High Warning Flag</b>	This can be either true or false, depending on the Current Temperature value displayed above.
<b>Voltage High Warning Flag</b>	This can be either true or false, depending on the Current Voltage value displayed above.
<b>Tx Bias High Warning Flag</b>	This can be either true or false, depending on the Tx bias current value displayed above.
<b>Tx Power High Warning Flag</b>	This can be either true or false, depending on the Current Tx power value displayed above.
<b>Rx Power High Warning Flag</b>	This can be either true or false, depending on the Current Tx power value displayed above.
<b>Temperature Low Warning Flag</b>	This can be either true or false, depending on the Current Temperature value displayed above.
<b>Voltage Low Warning Flag</b>	This can be either true or false, depending on the Current Voltage value displayed above.
<b>Tx Bias Low Warning Flag</b>	This can be either true or false, depending on the present Tx bias current value displayed above.

Line	Description
<b>Tx Power Low Warning Flag</b>	This can be either true or false, depending on the Current Tx power value displayed above.
<b>Rx Power Low Warning Flag</b>	This can be either true or false, depending on the Current Rx power value displayed above.

### Example

```

Dell#show interfaces tengigabitethernet 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](#) — displays the switch type, components (including media), the Dell Networking OS version including hardware identification numbers, and configured protocols.

## show range

Display all interfaces configured using the `interface range` command.

**Syntax** `show range`

**Command Modes** INTERFACE RANGE (config-if-range)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```

Dell(conf-if-range-te-0/6)#show range
interface tengigabitethernet 0/6
Dell(conf-if-range-te-0/6)#

```

### 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** `shutdown`

To activate an interface, use the `no shutdown` command.

**Defaults** The interface is disabled.

**Command Modes** INTERFACE

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> <tr> <td><b>8.3.17.0</b></td> <td>Supported on the M I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Version</b>	<b>Description</b>								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.								
<b>Usage Information</b>	<p>The <code>shutdown</code> command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the <code>show ip interface</code> command. Disabled interfaces are listed as down.</p> <p>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 <code>shutdown</code> 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, you must enter <code>no shutdown</code> on the port channel interface and at least one interface within that port channel.</p> <p>The <code>shutdown</code> and <code>description</code> commands are the only commands that you can configure on an interface that is a member of a port channel.</p>								
<b>Related Commands</b>	<p><a href="#">vlan tagged</a> — Test the condition of copper cables on 100/1000/10G Base-T modules.</p> <p><a href="#">interface vlan</a> — Creates a VLAN.</p> <p><a href="#">show ip interface</a> — Displays the interface routing status. Add the keyword <code>brief</code> to display a table of interfaces and their status.</p>								

## speed (for 1000/10000/auto interfaces)

Set the speed for 1000/10000 Base-T Ethernet interfaces. Set both sides of a link to the same speed (1000/10000) or to auto or the link may not come up.

<b>Syntax</b>	<code>speed {1000   10000   auto}</code>						
	To return to the default setting, use the <code>no speed {1000   10000   auto}</code> command.						
<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b>1000</b></td> <td>Enter the keyword <code>1000</code> to set the interface's speed to 1000 Mb/s.</td> </tr> <tr> <td style="vertical-align: top;"><b>10000</b></td> <td>Enter the keyword <code>10000</code> to set the interface's speed to 10000 Mb/s. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code>.</td> </tr> <tr> <td style="vertical-align: top;"><b>auto</b></td> <td>Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code>.</td> </tr> </table>	<b>1000</b>	Enter the keyword <code>1000</code> to set the interface's speed to 1000 Mb/s.	<b>10000</b>	Enter the keyword <code>10000</code> to set the interface's speed to 10000 Mb/s. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code> .	<b>auto</b>	Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code> .
<b>1000</b>	Enter the keyword <code>1000</code> to set the interface's speed to 1000 Mb/s.						
<b>10000</b>	Enter the keyword <code>10000</code> to set the interface's speed to 10000 Mb/s. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code> .						
<b>auto</b>	Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code> .						
<b>Defaults</b>	<b>auto</b>						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full-Switch						

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.10(0.0)</b></td> <td>Added support for fanned-out 1 Gigabit SFP port.</td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.10(0.0)</b>	Added support for fanned-out 1 Gigabit SFP port.	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>								
<b>9.10(0.0)</b>	Added support for fanned-out 1 Gigabit SFP port.								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.								
<b>Usage Information</b>	<p>This command is found on the 1000/10000 Base-T Ethernet interfaces.</p> <p>When you enable <code>auto</code>, the system performs an automatic discovery to determine the optics installed and configure the appropriate speed.</p> <p>When you configure a speed for the 1000/10000 interface, confirm the <code>negotiation auto</code> command setting. Both sides of the link must have auto-negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto-negotiation and you cannot change that setting.</p>								

If you use an active optical cable (AOC), you can convert the QSFP+ port to a 10 Gigabit SFP+ port or 1 Gigabit SFP port. You can use the `speed` command to enable the required speed.

#### Related Commands

- [negotiation auto](#) — enables or disables auto-negotiation on an interface.

## stack-unit portmode

Split a single 40G port into 4-10G ports on the switch.

**Syntax** `stack-unit stack-unit-number port number portmode quad`

**Parameters**

<b><i>stack-unit</i></b>	Enter the stack member unit identifier of the stack member to reset. The range is 0 to 5.
	<b>NOTE:</b> The switch commands accept Unit ID numbers from 0 to 5, though the switch supports stacking up to three units only with the Dell Networking OS version 8.3.7.1.
<b><i>number</i></b>	Enter the port number of the 40G port to be split. Enter one of the following port numbers for the switch: 48, 52, 56, or 60.

**Defaults** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

Splitting a 40G port into 4x10G port is supported on standalone and stacked units.

- You cannot use split ports as stack-link to stack a switch.
- The split ports switch unit cannot be a part of any stacked system.
- The unit number with the split ports must be the default (stack-unit 0).
- This set up can be verified using `show system brief` command. If the unit ID is different than 0, it must be renumbered to 0 before ports are split by using the `stackunit id renumber 0` command in EXEC mode.

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.

The system must be reloaded after issuing the CLI for the change to take effect.

## wavelength

Set the wavelength for tunable 10-Gigabit SFP+ optics.

**Syntax** `wavelength`  
To retain the existing wavelength, use the `no wavelength` command.

**Defaults** none

**Command Modes** INTERFACE

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



Version	Description
9.10(0.0)	Introduced on the S6000, S6000-ON, S5000, S4810, S4820T, S3048-ON, S4048-ON, M I/O Aggregator, FN I/O Module, MXL, C9010, S3100 series, and Z9100-ON.

**Usage Information**

The wavelength can be configured only on a tunable 10-Gigabit SFP+ optic. The wavelength range is from 1528.3 nm to 1568.77nm.

If you configure the wavelength on a non-tunable optic, there is no change to the existing wavelength. The configured wavelength is saved in the running configuration and is applicable, when a tunable optic is used.

If you do not configure the wavelength on an inserted tunable optic, the existing wavelength is used.

**Example**

The following example shows the wavelength set for a tunable 10-Gigabit SFP+ optic:

**Related Commands**

- `show config` — displays the interface configuration.

## 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 Aggregator, the maximum port channel ID is 128 and the maximum members per port channel is 4.

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.

**NOTE:** 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 PowerEdge FN I/O Aggregator Configuration Guide*

### channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

**Syntax**

`channel-member interface`

To delete an interface from a Port Channel, use the `no channel-member interface` command.

**Parameters**

**interface** (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults**

Not configured.

**Command Modes**

INTERFACE PORTCHANNEL

**Supported Modes**

Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

**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.

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 add up to 16 interfaces to a Port Channel on the switch. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 10-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

[interface port-channel](#) — creates a Port Channel interface.

## 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**

<b>group_number</b>	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
<b>port-channel number</b>	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)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## Example

```
Dell(conf)#port-channel failover-group
Dell(conf-po-failover-grp)#group 1 port-channel 1 port-channel 2
Dell(conf-po-failover-grp)#
```

## 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 physical interfaces on the Aggregator.

<b>Syntax</b>	<code>interface port-channel <i>channel-number</i></code> To delete a Port Channel, use the <code>no interface port-channel <i>channel-number</i></code> command.
<b>Parameters</b>	<b><i>channel-number</i></b> For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
<b>Defaults</b>	Not configured.
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch


<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, the 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 .

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, you must configure all members of a Port Channel 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**

- [interface](#) — configures a physical interface.
- [interface vlan](#) — configures a VLAN.

## 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.

<b>Syntax</b>	<code>minimum-links <i>number</i></code>
<b>Parameters</b>	<b><i>number</i></b> 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 <b>1</b> .
<b>Defaults</b>	<b>1</b>
<b>Command Modes</b>	INTERFACE
<b>Supported Modes</b>	Programmable-Mux (PMUX)

Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This feature groups two LAGs to work in tandem as a supergroup. For example, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For more information, refer to the *Port Channel* chapter in the *Dell Networking OS Configuration Guide*.

**Related Command**

[group](#) — groups two LAGs in a supergroup (“fate-sharing group”).  
[show interfaces port-channel](#) — displays information on configured Port Channel groups.

## show config

Display the current configuration of the selected LAG.

**Syntax** `show config`

**Command Modes** INTERFACE PORTCHANNEL

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell(conf-if-po-1)#show config
!
interface Port-channel 1
  no ip address
  shutdown
Dell(conf-if-po-1)#
```

## show interfaces port-channel

Display information on configured Port Channel groups.

**Syntax** `show interfaces port-channel [channel-number] [brief|description]`

**Parameters**

- channel-number** For a Port Channel interface, enter the keyword `port-channel` followed by a number. The range is from 1 to 128.
- brief** (OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.
- description** (OPTIONAL) Enter the keyword `description` to display interface information with description.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- For port-channel interfaces, you can specify multiple ports as `port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces port-channel 1 - 4`.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	9.7(0.0)	Introduced on the M I/O Aggregator.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**Usage Information** The following describes the `show interfaces port-channel` command shown in the following example.

Field	Description
<b>Port-Channel 1...</b>	Displays the status of LAG. In the Example, the status of the LAG, LAG fate-sharing group ("Failover-group") is listed.
<b>Hardware is...</b>	Displays the interface's hardware information and its assigned MAC address.
<b>Port-channel is part...</b>	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
<b>Internet address...</b>	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
<b>MTU 1554...</b>	Displays link and IP MTU.
<b>LineSpeed</b>	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
<b>Members in this...</b>	Displays the interfaces belonging to this port channel.
<b>ARP type:...</b>	Displays the ARP type and the ARP timeout value for the interface.

Field	Description
<b>Last clearing...</b>	Displays the time when the <code>show interfaces</code> counters were cleared.
<b>Queueing strategy.</b>	States the packet queuing strategy. FIFO means first in first out.
<b>packets input...</b>	Displays the number of packets and bytes into the interface.
<b>Input 0 IP packets...</b>	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.
<b>0 64-byte...</b>	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
<b>Received 0...</b>	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
<b>Output 0...</b>	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
<b>Rate information...</b>	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
<b>Time since...</b>	Displays the time since the last change in the configuration of this interface.

### Example (EtherScale)

```
Dell#show interfaces port-channel
Port-channel 1 is down, line protocol is down
Hardware address is 00:1e:c9:f1:00:05, Current address is
00:1e:c9:f1:00:05
Interface index is 1107755009
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :lag1001ec9f10005
MTU 12000 bytes, IP MTU 1500 bytes
LineSpeed auto
Members in this channel:
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:28:00
Queueing strategy: fifo
Input Statistics:
0 packets, 0 bytes
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts
0 runts, 0 giants, 0 throttles
0 CRC, 0 overrun, 0 discarded
Output Statistics:
0 packets, 0 bytes, 0 underruns
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 throttles, 0 discarded, 0 collisions
```

**User Information** The following describes the `show interfaces port-channel brief` command shown in the following example.

Field	Description
<b>LAG</b>	Lists the port channel number.
<b>Mode</b>	Lists the mode: <ul style="list-style-type: none"> <li>• L3 — for Layer 3</li> <li>• L2 — for Layer 2</li> </ul>
<b>Status</b>	Displays the status of the port channel. <ul style="list-style-type: none"> <li>• down — if the port channel is disabled (<code>shutdown</code>)</li> <li>• up — if the port channel is enabled (<code>no shutdown</code>)</li> </ul>

Field	Description
<b>Uptime</b>	Displays the age of the port channel in hours:minutes:seconds.
<b>Ports</b>	Lists the interfaces assigned to this port channel.
<b>(untitled)</b>	Displays the status of the physical interfaces (up or down). <ul style="list-style-type: none"> <li>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.</li> <li>In Layer 3 port channels, the primary port is not indicated.</li> </ul>

### Example

```
Dell#show int po bri
Codes: L - LACP Port-channel
       O - OpenFlow Controller Port-channel
       A - Auto Port-channel
       I - Internally Lagged
LAG Mode Status Uptime Ports
L    128 L3 down 00:00:00
Dell#
```

To indicate the LACP fallback, `Internally lagged` is added to the list. When the LAG auto-configures itself, the LAG status describes as 'I'.

### Related Commands

[show lacp](#) — displays the LACP matrix.

## Time Domain Reflectometer (TDR) Commands

TDR is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000/10G Base-T modules.

- [tdr-cable-test](#)
- [show tdr](#)

### Important Points to Remember

- The interface and port must be enabled (configured—see the `interface` command) before running TDR. An error message is generated if you have not enabled the interface.
- The interface on the far-end device must be shut down before running TDR.
- Because TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

### tdr-cable-test

Test the condition of copper cables on 100/1000/10GBase-T modules.

**Syntax** `tdr-cable-test interface`

**Parameters** *interface* Enter the keyword `TenGigabitEthernet` followed by the slot/port information for the 100/1000/10GBase-T Ethernet interface.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

#### Usage Information

The interface must be enabled to run the test or an error message is generated:

#### Related Commands

[show tdr](#) — Displays the results of the TDR test.

## show tdr

Displays the TDR test results.

#### Syntax

`show tdr interface`

#### Parameters

**interface** Enter the keyword `TenGigabitEthernet` followed by the slot/port information for the 100/1000/10 GbaseT Ethernet interface.

#### Defaults

none

#### Command Modes

EXEC

#### Supported Modes

All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

#### Usage Information

If the TDR test has not been run, an error message is generated:

```
%Error: Please run the TDR test first
```

The following describes the TDR test status.

Status	Definition
<b>OK Status: Terminated</b>	TDR test is complete, no fault is detected on the cable, and the test is terminated.
<b>Length: 92 (+/- 1) meters, Status: Shorted</b>	A short is detected on the cable. The location, in this Example is 92 meters. The short is accurate to plus or minus one meter.
<b>Length: 93 (+/- 1) meters, Status: Open</b>	An opening is detected on the cable. The location, in this Example is 93 meters. The open is accurate to plus or minus one meter.
<b>Status: Impedance Mismatch</b>	There is an impedance mismatch in the cables.

#### Example

#### Related Commands

[tdr-cable-test](#) — Runs the TDR test.

## Enhanced Validation of Interface Ranges

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`



2/0-1, te 10/0, fa 0/0, 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.

## UDP Broadcast

The user datagram protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

### Important Points to Remember

- Routing information protocol (RIP) is not supported with the UDP Broadcast feature.
- If you configure this feature on an interface using the `ip udp-helper udp-port` command, the `ip directed-broadcast` command becomes ineffective on that interface.
- The existing `show interface` command has been modified to display the configured broadcast address.

### debug ip udp-helper

Enable UDP debug and display the debug information on a console.

**Syntax** `debug ip udp-helper`  
To disable debug information, use the `no debug ip udp-helper` command.

**Defaults** Debug disabled.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Te 4/1 with IP DA (0xffffffff) will be sent on Te
4/2 Te 4/3
Vlan 3

01:44:54: Pkt rcvd on Te 5/1 is handed over for DHCP processing.
```

#### Related Commands

- [ip udp-broadcast-address](#) — configures a UDP IP address for broadcast.
- [ip udp-helper udp-port](#) — enables the UDP broadcast feature on an interface.
- [show ip udp-helper](#) — displays the configured UDP helper(s) on all interfaces.

### ip udp-broadcast-address

Configure an IP UDP address for broadcast.

**Syntax** `ip udp-broadcast-address address`  
To delete the configuration, use the `no ip udp-broadcast-address address` command.

<b>Parameters</b>	<b><i>address</i></b>	Enter an IP broadcast address in dotted decimal format (A.B.C.D).
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	INTERFACE (config-if)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Enter an IP broadcast address in dotted decimal format (A.B.C.D).
<b>Usage Information</b>	When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet's IP destination address is replaced with the configured broadcast address.	
<b>Related Commands</b>	<a href="#">debug ip udp-helper</a> — enables debug and displays the debug information on a console. <a href="#">show ip udp-helper</a> — displays the configured UDP helpers on all interfaces.	

## ip udp-helper udp-port

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

<b>Syntax</b>	<code>ip udp-helper udp-port [<i>udp-port-list</i>]</code>	
	To disable the UDP broadcast on a port, use the <code>no ip udp-helper udp-port [<i>udp-port-list</i>]</code> command.	
<b>Parameters</b>	<b><i>udp-port-list</i></b>	(OPTIONAL) Enter up to 16 comma-separated UDP port numbers.  <b>NOTE:</b> If you do not use this option, all UDP ports are considered by default.
<b>Defaults</b>	none	
<b>Command Modes</b>	INTERFACE (config-if)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>If you configure the <code>ip helper-address</code> command and <code>ip udp-helper udp-port</code> command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server per the <code>ip helper-address</code> configuration. This occurs regardless if the <code>ip udp-helper udp-port</code> command contains port numbers 67/68 or not.</p> <p>If you only configure the <code>ip udp-helper udp-port</code> command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the <code>udp-port-list</code>.</p>	
<b>Related Commands</b>	<a href="#">ip helper-address</a> — configures the destination broadcast or host address for the DHCP server. <a href="#">debug ip udp-helper</a> — enables debug and displays the debug information on a console. <a href="#">show ip udp-helper</a> — displays the configured UDP helpers on all interfaces.	

## show ip udp-helper

Display the configured UDP helpers on all interfaces.

**Syntax** `show ip udp-helper`

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ip udp-helper
-----
Port      UDP  port  list
-----
Te 1/1    656, 658
Te 1/2    All
```

### Related Commands

[debug ip udp-helper](#) — enables debug and displays the debug information on a console.

[ip udp-broadcast-address](#) — configures a UDP IP address for broadcast.

[ip udp-helper udp-port](#) — enables the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

## Port Interface Commands

The following commands are for physical, loopback, and null interfaces:

- [clear counters](#)
- [clear mac-address-table dynamic](#)
- [interface range](#)
- [interface vlan](#)
- [keepalive](#)
- [name](#)
- [show config \(INTERFACE mode\)](#)
- [show config \(from INTERFACE RANGE mode\)](#)
- [show config \(from INTERFACE VLAN mode\)](#)
- [show interfaces configured](#)
- [show interfaces description](#)
- [show interfaces stack-unit](#)
- [show interfaces port-channel](#)
- [show interfaces status](#)
- [show interfaces switchport](#)
- [show vlan](#)
- [shutdown](#)
- [speed \(for 1000/10000 interfaces\)](#)

## Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual local area networks (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address only on the default VLAN. FTP, TFTP, ACLs, and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple VLANs, state of a VLAN interface may continually switch between Master and Backup.

- [auto vlan](#)
- [default vlan-id](#)
- [name](#)
- [show config \(from INTERFACE VLAN mode\)](#)
- [show vlan](#)
- [vlan tagged](#)
- [vlan untagged](#)

## auto vlan

Change the port to auto or admin vlan mode (enable or disable all auto VLANs).

<b>Syntax</b>	<code>auto vlan</code>	
		To remove membership from 4K VLAN, use the <code>no auto vlan</code> command.
<b>Defaults</b>	none	
<b>Parameters</b>	<b>description</b>	Enter a text string description to identify the VLAN (80 characters maximum).
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Standalone Mode	
<b>Usage Information</b>	The <code>auto vlan</code> command adds the port as untagged to default vlan and tagged to all other 4094 VLAN.	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## clear mac-address-table dynamic

Clear the MAC address table of all MAC addresses learned dynamically.

<b>Syntax</b>	<code>clear mac-address-table dynamic {interface tengigabitethernet slot/port-id}</code>	
<b>Parameters</b>	<b>interface</b>	Enter the keyword <code>interface range</code> and one of the interfaces — <code>slot/port</code> , <code>port-channel</code> or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges-spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces.  Slot/Port information must contain a space before and after the dash. For example, <code>interface range tengigabitethernet 0/1 - 5</code> is valid; <code>interface range tengigabitethernet 0/1-5</code> is not valid. <ul style="list-style-type: none"><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li></ul>
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## default vlan-id

Set the default VLAN ID.

<b>Syntax</b>	<code>default vlan-id &lt;vlan-id&gt;</code> To reset the default VLAN ID, use the <code>no default vlan-id</code> command.						
<b>Defaults</b>	none						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	All Modes						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td><b>8.3.17.0</b></td><td>Supported on the M I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
Version	Description						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.						
<b>Related commands</b>	<a href="#">show vlan</a> — Displays VLAN configuration.						

## feature fc

Enables the Fibre channel communication via the NPG functionality.

<b>Syntax</b>	<code>feature fc</code>				
<b>Command Modes</b>	CONFIGURATION				
<b>Default</b>	Enabled				
<b>Supported Modes</b>	Programmable-Mux (PMUX)				
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.6(0.0)</b></td><td>Supported on the FN 2210S Aggregator and M I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator and M I/O Aggregator.
Version	Description				
<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator and M I/O Aggregator.				

## monitor interface

Monitor counters on a single interface or all interfaces on a stack unit. The screen is refreshed every five seconds and the CLI prompt disappears.

<b>Syntax</b>	<code>monitor interface [interface]</code> To disable monitoring and return to the CLI prompt, press the <code>q</code> key.				
<b>Parameters</b>	<p><b><i>interface</i></b> (OPTIONAL) Enter the following keywords and slot/port or number information:</p> <ul style="list-style-type: none"><li>• For the management port, enter the keyword <code>managementethernet</code> followed by the slot (0) and the port (0).</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li><li>• For a Port Channel interface, enter the keyword <code>port-channel</code> followed by a number. The range is from 1 to 128.</li></ul>				
<b>Command Modes</b>	<ul style="list-style-type: none"><li>• EXEC</li><li>• EXEC Privilege</li></ul>				
<b>Supported Modes</b>	All Modes				
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
Version	Description				
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.				

## Usage Information

The delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

Key	Description
<b>systest-3</b>	Displays the host name assigned to the system.
<b>monitor time</b>	Displays the amount of time since the <code>monitor interface</code> command was entered.
<b>time</b>	Displays the amount of time the chassis is up (since last reboot).
<b>m</b>	Change the view from a single interface to all interfaces on the stack unit or visa-versa.
<b>c</b>	Refresh the view.
<b>b</b>	Change the counters displayed from Packets on the interface to Bytes.
<b>r</b>	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
<b>l</b>	Change the view to the next interface on the stack unit, or if in the stack unit mode, the next stack unit in the chassis.
<b>a</b>	Change the view to the previous interface on the stack unit, or if in line stack unit mode, the previous stack unit in the chassis.
<b>T</b>	Increase the screen refresh rate.
<b>t</b>	Decrease the screen refresh rate.
<b>q</b>	Return to the CLI prompt.

## Example (Single Interface)

```
systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time: 03:26:26
Interface: tengig 0/3, 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
```

## 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]
  Gi 0/0   Down      0          0          0
  Gi 0/1   Down      0          0          0
  Gi 0/2   Up        61512      52        66160      42
```

```

Gi 0/3 Up 63086 20 9405888 24
Gi 0/4 Up 14697471418 2661481 13392989657
2661385
Gi 0/5 Up 3759 3 161959604 832816
Gi 0/6 Up 4070 3 8680346 5
Gi 0/7 Up 61934 34 138734357 72
Gi 0/8 Up 61427 1 59960 1
Gi 0/9 Up 62039 53 104239232 3
Gi 0/10 Up 17740044091 372 7373849244 79
Gi 0/11 Up 18182889225 44 7184747584 138
Gi 0/12 Up 18182682056 0 3682 1
Gi 0/13 Up 18182681434 43 6592378911 144
Gi 0/14 Up 61349 55 86281941 15
Gi 0/15 Up 59808 58 62060 27
Gi 0/16 Up 59889 1 61616 1
Gi 0/17 Up 0 0 14950126 81293
Gi 0/18 Up 0 0 0 0
Gi 0/19 Down 0 0 0 0
Gi 0/20 Up 62734 54 62766 18
Gi 0/21 Up 60198 9 200899 9
Gi 0/22 Up 17304741100 3157554 10102508511
1114221
Gi 0/23 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

```

## name

Assign a name to the Default VLAN.

**Syntax** `namevlan-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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This CLI applies only to the Default VLAN.

To display information about a named VLAN, enter the `show vlan` command with the `name` parameter or the `show interfaces description` command.

- Related commands**
- [default vlan-id](#) — Assigns a descriptive text string to the interface.
  - [interface vlan](#) — Configures a VLAN.
  - [show vlan](#) — Displays the current VLAN configurations on the switch.

## show config (INTERFACE mode)

Displays the interface configuration.

**Syntax** `show config`

**Command Modes** INTERFACE

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### Example

## show config (from INTERFACE VLAN mode)

Displays the current configuration of the Default VLAN.

**Syntax** show config

**Command Modes** INTERFACE VLAN

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### Example

```
Dell(conf-if-vl-1)#show config
!
interface Vlan 1
description a
no ip address
mtu 2500
shutdown
Dell(conf-if-vl-1)#
```

## show config (from PROTOCOL LLDP mode)

Displays the LLDP configuration.

**Syntax** show config

**Command Modes** PROTOCOL LLDP

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### Example

```
Dell(conf-lldp)#show conf
!
protocol lldp
Dell(conf-lldp)#
```



# show vlan

Displays the current VLAN configurations on the switch.

**Syntax** `show vlan [brief | id vlan-id | name vlan-name]`

**Parameters**

- brief** (OPTIONAL) Enter the keyword `brief` to display the following information:
  - VLAN ID
  - VLAN name (left blank if none is configured.)
  - Spanning Tree Group ID
  - MAC address aging time
  - IP address
- id *vlan-id*** (OPTIONAL) Enter the keyword `id` followed by a number from 1 to 4094. Only information on the VLAN specified is displayed
- name *vlan-name*** (OPTIONAL) Enter the keyword `name` followed by the name configured for the VLAN. Only information on the VLAN named is displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information** The following describes the `show vlan` command information given in the following example

Column Heading	Description
<b>(Column 1 — no heading)</b>	<ul style="list-style-type: none"><li>• asterisk symbol (*) = Default VLAN</li><li>• G = GVRP VLAN</li><li>• P = primary VLAN</li><li>• C = community VLAN</li><li>• I = isolated VLAN</li></ul>
<b>NUM</b>	Displays existing VLAN IDs.
<b>Status</b>	Displays the word Inactive for inactive VLANs and the word Active for active VLANs.
<b>Q</b>	Displays G for GVRP tagged, M for member of a VLAN-Stack VLAN, T for tagged interface, U (for untagged interface), x (uncapitalized x) for Dot1x untagged, or X (capitalized X) for Dot1x tagged.
<b>Ports</b>	

## Example

```
Dell# show vlan id 40
Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring
VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
x - Dot1x untagged, X - Dot1x tagged
G - GVRP tagged, M - Vlan-stack, H - VSN tagged
i - Internal untagged, I - Internal tagged, v - VLT untagged, V
- VLT tagged
NUM Status Description Q Ports
1 Inactive a
Dell#
```

### Example (Brief)

```
Dell#show vlan brief
VLAN Name                               STG MAC Aging   IP Address
-----
1                                         0    0          unassigned
2                                         0    0          unassigned
20                                        0    0          unassigned
1002                                     0    0          unassigned
Dell#
```

### Example (Using a VLAN Name)

```
Dellconf)#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 TenGig 1/22
Dell(conf-if-vl-222)#
Dell#
```

### Related Commands

[interface vlan](#) — Configures a VLAN.

## speed (for 1000/10000 interfaces)

Set the speed for 1000/10000 interfaces. Both sides of a link must be set to the same speed (1000/10000) or to auto or the link may not come up.

**Syntax** `speed {1000 | 10000 | auto}`

To return to the default setting, use the `no speed {1000 | 10000 | auto}` command.

### Parameters

<b>1000</b>	Enter the keyword <code>1000</code> to set the interface's speed to 1000 Mb/s.
<b>10000</b>	Enter the keyword <code>10000</code> to set the interface's speed to 10000 Mb/s. Auto-negotiation is enabled.
<b>auto</b>	Enter the keyword <code>auto</code> to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to <code>name</code> .

**Defaults** `auto`

**Command Modes** INTERFACE

**Supported Modes** All Modes

### Command History

Version	Description
<b>9.10(0.0)</b>	Added support for fanned-out 1 Gigabit SFP port.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Usage Information

This command is found on the 1000/10000 Base-T Ethernet interfaces.

When you enable `auto`, the system performs an automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 1000/10000 interface, confirm the `negotiation auto` command setting. Both sides of the link must have auto-negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto-negotiation and you cannot change that setting.

If you use an active optical cable (AOC), you can convert the QSFP+ port to a 10 Gigabit SFP+ port or 1 Gigabit SFP port. You can use the `speed` command to enable the required speed.

## Related Commands

# stack-unit port-group port mode ethernet

Converts the interfaces 9 and 10 from Fibre Channel mode to Ethernet.

**Syntax** `stack-unit unit number port-group 0 portmode ethernet`

To convert the interfaces 9 and 10 from Ethernet to Fibre Channel mode, use the `no stack-unit unit number port-group 0 portmode ethernet`.

**Parameters**

<b>stack-unit</b>	Enter the keyword <code>stack-unit</code> followed by a stack member number to select the stack unit. The range is 0 to 5.
<b>port-group</b>	Enter the keyword <code>port-group</code> followed by 0.
<b>portmode ethernet</b>	Enter the keyword <code>portmode ethernet</code> to convert the interfaces from Fibre Channel mode to Ethernet.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.6(0.0)</b>	Supported on the FN2210S Aggregator.

# vlan tagged (CMC)

Add a Layer 2 interface to a VLAN as a tagged interface.

**Syntax** `vlan tagged [vlan-id]`

To remove a tagged interface from a VLAN, use the `no vlan tagged vlan-id` command.

**Parameters**

<b>vlan-id</b>	Enter the VLAN ID. The range is from 1 to 4094.
----------------	---

**Defaults** **All interfaces in Layer 2 mode are untagged.**

**Command Modes** INTERFACE

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** If the interface belongs to several VLANs, you must 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.

When two or more ports configured for VLANs form a LAG, the resulting LAG is a tagged member of all the configured VLANs and an untagged member of the VLAN to which the port with the lowest port ID belongs.

For example, if port 0/1-32 is an untagged member of VLAN 2 and port 0/41 is an untagged member of VLAN 3, the resulting LAG consisting of the two ports is an untagged member of VLAN 2 and a tagged member of VLAN3.

### Example

```
Dell(conf-if-te-0/2)#vlan tagged ?
VLAN-RANGE          Comma/Hyphen separated VLAN ID set
Dell(conf-if-te-0/2)#vlan tagged 2,3-4
Dell(conf-if-te-0/2)#show config
!
interface TenGigabitEthernet 0/2
mtu 12000
vlan tagged 2-4
!
port-channel-protocol LACP
port-channel 1 mode active
!
protocol lldp
advertise management-tlv system-name
dcbx port-role auto-downstream
no shutdown
Dell(conf-if-te-0/2)#
```

### Related Commands

[interface vlan](#) — Configures a VLAN.

[vlan untagged](#) — Specifies which interfaces in a VLAN are untagged.

## vlan untagged (CMC)

Add a Layer 2 interface to a VLAN as an untagged interface.

**Syntax** `vlan untagged [vlan-id]`

To remove a untagged interface from a VLAN, use the `no vlan untagged [vlan-id]` command.

**Parameters** *vlan-id* Enter the VLAN ID. The range is from 1 to 4094.

**Defaults** All interfaces in Layer 2 mode are untagged.

**Command Modes** INTERFACE

**Supported Modes** All Modes

### Command History

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

### 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 vlan tagged` command.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

When two or more ports configured for VLANs form a LAG, the resulting LAG is a tagged member of all the configured VLANs and an untagged member of the VLAN to which the port with the lowest port ID belongs.

For example, if port 0/33 is an untagged member of VLAN 2 and port 0/41 is an untagged member of VLAN 3, the resulting LAG consisting of the two ports is an untagged member of VLAN 2 and a tagged member of VLANs 2 and 3.

## Example

```
Dell(conf-if-te-0/2)#vlan untagged ?
<1-4094> Untagged VLAN id
Dell(conf-if-te-0/2)#
Dell(conf-if-te-0/2)#vlan untagged 4094
Dell(conf-if-te-0/2)#show config
!
interface TenGigabitEthernet 0/2
mtu 12000
vlan untagged 4094
!
port-channel-protocol LACP
port-channel 1 mode active
!
protocol lldp
advertise management-tlv system-name
dcbx port-role auto-downstream
no shutdown
Dell(conf-if-te-0/2)#
```

## Related Commands

[interface vlan](#) — Configures a VLAN.

[vlan tagged](#) — Specifies which interfaces in a VLAN are tagged.

# IPv4 Routing

The aggregator supports both IPv4 and IPv6 routing and these are used only for the management purpose.

This chapter describes the IPv4 related commands. They are:

- `clear tcp statistics`
- `debug ip dhcp`
- `debug ip icmp`
- `show ip management-route`
- `show ip multicast-cam stack-unit`
- `show ip interface`
- `show ip route`
- `show tcp statistics`

## Topics:

- `arp`
- `arp learn-enable`
- `arp retries`
- `arp timeout`
- `clear arp-cache`
- `clear host`
- `clear ip fib stack-unit`
- `clear ip route`
- `clear tcp statistics`
- `debug arp`
- `debug ip dhcp`
- `debug ip icmp`
- `debug ip packet`
- `icmp6-redirect enable`
- `ip address`
- `ip directed-broadcast`
- `ip domain-list`
- `ip domain-lookup`
- `ip domain-name`
- `ip helper-address`
- `ip helper-address hop-count disable`
- `ip host`
- `ip icmp source-interface`
- `ipv6 icmp source-interface`
- `ip max-frag-count`
- `ip name-server`
- `ip proxy-arp`
- `ip route`
- `ip source-route`
- `ip tcp initial-time`
- `show ip tcp initial-time`
- `ip unreachable`
- `management route`
- `show arp`
- `show arp retries`
- `show hosts`
- `show ip cam stack-unit`

- [show ip fib stack-unit](#)
- [show ip interface](#)
- [show ip management-route](#)
- [show ip multicast-cam stack-unit](#)
- [show ip protocols](#)
- [show ip route](#)
- [show ip route list](#)
- [show ip route summary](#)
- [show ip traffic](#)
- [show tcp statistics](#)

## arp

To associate an IP address with a multicast MAC address in the switch when you configure multicast mode of the network load balancing (NLB), use the address resolution protocol (ARP).

**Syntax** `arp ip-address multicast-mac-address interface`

To remove an ARP address, use the `no arp ip-address` command.

<b>Parameters</b>	<b><i>ip-address</i></b>	Enter an IP address in dotted decimal format.
	<b><i>multicast-mac-address</i></b>	Enter a 48-bit hexadecimal address in MAC address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic..
	<b><i>interface</i></b>	Enter any of the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0.</li> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• 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.</li> </ul>

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Added the support for association of an IP address with multicast MAC address on the MXL platform.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 `arp ip-address multicast-mac-address` 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.

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.

Although static ARP entries take precedence over dynamically-learned ARP entries, a static ARP entry that points to a wrong port is not included in the FIB or ARP entries.

**Related Commands**      [clear arp-cache](#) — clears dynamic ARP entries from the ARP table.  
[show arp](#) — displays the ARP table.

## arp learn-enable

Enable ARP learning using gratuitous ARP.

**Syntax**                  `arp learn-enable`

**Defaults**                Disabled

**Command Modes**      CONFIGURATION

**Supported Modes**    Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**                  `arp retries number`

**Parameters**            *number*                  Enter the number of retries. The range is from 5 to 20. The default is **5**.

**Defaults**                **5**

**Command Modes**      CONFIGURATION

**Supported Modes**    Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**            *minutes*                  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

**Supported Modes**    Full-Switch



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [interface | ip ip-address] [no-refresh]`

Parameters	Parameter	Description
	<b><i>interface</i></b>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0.</li> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
	<b><i>ip ip-address</i></b>	(OPTIONAL) Enter the keyword <code>ip</code> then the IP address of the ARP entry you wish to clear.
	<b><i>no-refresh</i></b>	(OPTIONAL) Enter the keywords <code>no-refresh</code> to delete the ARP entry from CAM. Or use this option with <i>interface</i> or <i>ip ip-address</i> to specify which dynamic ARP entries you want to delete.
		<b>NOTE:</b> 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

**Supported Modes**     Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear host

Remove one or all dynamically learned host table entries.

**Syntax**     `clear host name`

Parameters	Parameter	Description
	<b><i>name</i></b>	Enter the name of the host to delete. Enter * to delete all host table entries.

**Command Modes**     EXEC Privilege

**Supported Modes**     Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip fib stack-unit

Clear all forwarding information base (FIB) entries in the specified stack unit (use this command with caution, refer to *Usage Information*.)

<b>Syntax</b>	<code>clear ip fib stack-unit <i>unit-number</i></code>	
<b>Parameters</b>	<b><i>unit-number</i></b>	Enter the number of the stack unit. The range is from 0 to 5.
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To clear Layer 3 CAM inconsistencies, use this command.  
 **CAUTION: Executing this command causes traffic disruption.**

**Related Commands** [show ip fib stack-unit](#) — shows FIB entries.

## clear ip route

Clear one or all routes in the routing table.

<b>Syntax</b>	<code>clear ip route { *   <i>ip-address mask</i> }</code>	
<b>Parameters</b>	<b>*</b>	Enter an asterisk (*) to clear all learned IP routes.
	<b><i>ip-address mask</i></b>	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 the TCP counters.

**Syntax** `clear tcp statistics`

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

# debug arp

View information on ARP transactions.

**Syntax** `debug arp [interface] [count value]`

To stop debugging ARP transactions, use the `no debug arp` command.

<b>Parameters</b>	<b>interface</b>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0.</li><li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>
	<b>count value</b>	(OPTIONAL) Enter the keyword <code>count</code> then the count value. The range is from 1 to 65534.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 DHCP relay transactions and display the information on the console.

**Syntax** `debug ip dhcp`

**Parameters** **debug ip dhcp** To disable debug, use the `no debug ip dhcp` command.

**Defaults** Debug disabled  
**Command Mode** EXEC Privilege  
**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
FTOS#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
FTOS#
```

## 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 or number information:

- For the management interface, enter the keyword ManagementEthernet then the slot/port information. The slot range is 0 and the port range is 0.
- For a 10 Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

- For VLAN, enter the keyword `vlan` then by a number from 1 to 4094.

**count value**

(OPTIONAL) Enter the keywords `count` then the count value. The ranges from 1 to 65534. The default is **Infinity**.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information**

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

**Example**

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40:
```

## 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**

<b>access-group name</b>	Enter the keywords <code>access-group</code> then the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.
<b>count value</b>	(OPTIONAL) Enter the keyword <code>count</code> then the count value. The range is from 1 to 65534. The default is <b>Infinity</b> .
<b>interface</b>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For the Management interface, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 0 to 1 and the port range is 0.</li> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `debug ip packet` command in the following example.

Field	Description
<b>s=</b>	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
<b>d=</b>	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.
<b>len</b>	Displays the packet's length.
<b>sending, rcvd, fragment, sending broad/multicast proto, unroutable</b>	The last part of each line lists the status of the packet.
<b>TCP src=</b>	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
<b>UDP src=</b>	Displays the source and destination ports for the UDP packets.
<b>ICMP type=</b>	Displays the ICMP type and code.
<b>IP Fragment</b>	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of the original datagram.

## Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK
    PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226, sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK
    PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 1/8), len 64, sending broad/
multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 1/8), 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#
```

## icmp6-redirect enable

Enable ICMP and ICMP6 redirects.

**Syntax** `icmp6-redirect enable`

**Command Modes** EXEC Privilege

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

Version	Description
<b>Legacy command</b>	Legacy command

### Usage Information

Use this command to notify hosts on the same network that a better route is available for a specific destination.

The `icmp6-redirect enable` command is applicable for both IP and IPv6 routes.

## ip address

Assign a primary and secondary IP address to the interface.

**Syntax** `ip address ip-address mask [secondary]`

To delete an IP address from an interface, use the `no ip address [ip-address]` command.

Parameters		
<b>ip-address</b>		Enter an IP address in dotted decimal format.
<b>mask</b>		Enter the mask of the IP address in slash prefix format (for example, /24).
<b>secondary</b>		(OPTIONAL) Enter the keyword <code>secondary</code> to designate the IP address as the secondary address.

**Defaults** Not configured.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To fully enable DNS, also specify one or more domain name servers with the `ip name-server` command.

The 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

The 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 the system 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** `ip helper-address hop-count disable`  
To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.

**Defaults** Enabled; the hops field in the DHCP message header is incremented by default.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through the 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 IP address to be used by the host-to-IP address mapping table.

**Syntax** `ip host name ip-address`  
To remove an IP host, use the `no ip host name [ip-address]` command.

**Parameters**

<b><i>name</i></b>	Enter a text string to associate with one IP address.
<b><i>ip-address</i></b>	Enter an IP address, in dotted decimal format, to be mapped to the name.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# 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** ***interface*** Enter one of the following keywords and slot/port or number information:

- For a Management Ethernet interface, enter the keyword `managementethernet`.  
**i** **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 Loopback interface, enter the keyword `loopback`. 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.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet`.
- For a VLAN interface, enter the keyword `vlan`. The range is from 1 to 4094.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.3(0.0)	Introduced on the MXL platform.

### 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 0/1
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

***interface***

Enter one of the following keywords and slot/port 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 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 Loopback interface, enter the keyword `loopback`. 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.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet`.
- For a VLAN interface, enter the keyword `vlan`. The range is from 1 to 4094.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.3(0.0)	Introduced on the MXL platform.

#### 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 0/1
Dell(conf)#
```

## ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

**Syntax** `ip max-frag-count count`  
 To place no limit on the number of fragments allowed, use the `no ip max-frag-count` command.

**Parameters** **count** Enter a number for the number of fragments allowed for re-assembly. The range is from 2 to 256.

**Defaults** No limit is set on number of fragments allowed.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `ip name-server ipv4-address [ipv4-address2...ipv4-address6]`  
 To remove a name server, use the `no ip name-server ip-address` command.

**Parameters** **ipv4-address** Enter the IPv4 address, in dotted decimal format, of the name server to be used.  
**ipv4-address2...** (OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.  
**ipv4-address6**

**Defaults** No name servers are configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [show ip interface](#) — displays the interface routing status and configuration.

## ip route

Assign a static route to the switch.

**Syntax** `ip route destination mask {ip-address | interface [ip-address]}[distance]`  
To delete a specific static route, use the `no ip route destination mask {address | interface [ip-address]}` command.  
To delete all routes matching a certain route, use the `no ip route destination mask` command.

Parameters		
<b><i>destination</i></b>		Enter the IP address in dotted decimal format of the destination device.
<b><i>mask</i></b>		Enter the mask in the slash prefix format (/x) of the destination device's IP address.
<b><i>ip-address</i></b>		Enter the IP address in dotted decimal format of the forwarding router.
<b><i>interface</i></b>		For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.
<b><i>distance</i></b>		(OPTIONAL) Enter a number as the distance metric assigned to the route. The range is from 1 to 255.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						
<b>Usage Information</b>	<p>Using the following example of a static route: <code>ip route 33.33.33.0 /24 tengigabitethernet 0/0 172.31.5.43</code></p> <ul style="list-style-type: none"> <li>• 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 gig 0/0 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.</li> <li>• When the interface goes down, Dell Networking OS withdraws the route.</li> <li>• When the interface comes up, Dell Networking OS re-installs the route.</li> <li>• When recursive resolution is "broken," Dell Networking OS withdraws the route.</li> <li>• When recursive resolution is satisfied, Dell Networking OS re-installs the route.</li> </ul>						
<b>Related Commands</b>	<a href="#">show ip route</a> — views the switch routing table.						

## ip source-route

Enable the system 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

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

## ip tcp initial-time

Define the wait duration in seconds for the TCP connection to be established.

**Syntax** `ip tcp initial-time <8-75>`  
 To restore the default behavior, which causes the wait period to be set as eight seconds, use the `no ip tcp initial-time` command.

**Parameters** `<8-75>` Wait duration in seconds for the TCP connection to be established.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.3(0.0)</b></td> <td>Introduced on the MXL platform.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.3(0.0)</b>	Introduced on the MXL platform.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.3(0.0)</b>	Introduced on the MXL platform.						

**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.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module platform.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## management route

Configure a static route that points to the Management interface or a forwarding router.

**Syntax** `management route {ipv4-address | ipv6-address}/mask{forwarding-router-address | managementethernet}`

**Parameters**

- {ipv4-address | ipv6-address}/mask*** Enter an IPv4 address (A.B.C.D) or the IPv6 address followed by the prefix-length for the IP address of the management interface.
- forwarding-router-address*** Enter an IPv4 address of a forwarding router.
- managementethernet*** Enter the keyword `managementethernet` for the Management interface.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes



<b>Command History</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b>Version</b></td> <td style="vertical-align: top;"><b>Description</b></td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						
<b>Usage Information</b>	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 management routes. This command manages both tables.						

## show arp

Displays the ARP table.

<b>Syntax</b>	<code>show arp [interface <i>interface</i>] [dynamic] [summary]</code>	
<b>Parameters</b>	<b>interface</b> <b><i>interface</i></b>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For the Management interface, enter the keyword <code>managementethernet</code> followed by the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li> </ul>
	<b>dynamic</b>	(OPTIONAL) Enter the keyword <code>dynamic</code> to view dynamic entries.
	<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to view a summary of ARP entries.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b>Version</b></td> <td style="vertical-align: top;"><b>Description</b></td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						

**Usage Information** The following describes the `show arp` command shown in the following example.

<b>Row Heading</b>	<b>Description</b>
<b>Protocol</b>	Displays the protocol type.
<b>Address</b>	Displays the IP address of the ARP entry.
<b>Age(min)</b>	Displays the age (in minutes) of the ARP entry.
<b>Hardware Address</b>	Displays the MAC address associated with the ARP entry.
<b>Interface</b>	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
<b>VLAN</b>	Displays the VLAN ID, if any, associated with the ARP entry.
<b>CPU</b>	Lists which CPU the entries are stored on.

### Example

```
Dell#show arp
Protocol Address Age(min) Hardware Address Interface VLAN CPU
-----
Internet 10.11.8.6 167 00:01:e9:45:00:03 Ma 0/0 - CP
Internet 10.11.68.14 124 00:01:e9:45:00:03 Ma 0/0 - CP
Internet 10.11.209.254 0 00:01:e9:45:00:03 Ma 0/0 - 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 - V1 10 pv 200 CP
Internet 5.5.5.10      - 00:01:e8:44:99:55 - V1 10      CP
Internet 10.1.2.4      1 00:01:e8:d5:9e:e2 Ma 0/0      - CP
Internet 10.10.10.4   1 00:01:e8:d5:9e:e2 Ma 0/0      - CP
Internet 10.16.127.53 1 00:01:e8:d5:9e:e2 Ma 0/0      - CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2 Ma 0/0      - CP
Internet 133.33.33.4  1 00:01:e8:d5:9e:e2 Ma 0/0      - CP
```

### Usage Information

The following describes the `show arp summary` command shown in the following example.

#### Row Heading Description

<b>Total Entries</b>	Lists the total number of ARP entries in the ARP table.
<b>Static Entries</b>	Lists the total number of configured or static ARP entries.
<b>Dynamic Entries</b>	Lists the total number of learned or dynamic ARP entries.
<b>CPU</b>	Lists which CPU the entries are stored on.

### Example (Summary)

```
Dell#show arp summary
-----
TotalEntries Static Entries Dynamic Entries CPU
-----
3              0              3              CP
Dell#
```

## show arp retries

Display the configured number of ARP retries.

**Syntax** `show arp retries`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on MXL 10/40GbE Switch IO Module

**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

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show hosts` command in the following example.

Field	Description
<b>Default domain...</b>	Displays the domain name (if configured).
<b>Name/address lookup...</b>	States if DNS is enabled on the system. <ul style="list-style-type: none"><li>• If DNS is enabled, the Name/Address lookup is domain service.</li><li>• If DNS is not enabled, the Name/Address lookup is static mapping</li></ul>
<b>Name servers are...</b>	Lists the name servers, if configured.
<b>Host</b>	Displays the host name assigned to the IP address.
<b>Flags</b>	Classifies the entry as one of the following: <ul style="list-style-type: none"><li>• <code>perm</code> — the entry was manually configured and will not time out</li><li>• <code>temp</code> — the entry was learned and will time out after 72 hours of inactivity.</li></ul> Also included in the flag is an indication of the validity of the route: <ul style="list-style-type: none"><li>• <code>ok</code> — the entry is valid.</li><li>• <code>ex</code> — the entry expired.</li><li>• <code>??</code> — the entry is suspect.</li></ul>
<b>TTL</b>	Displays the amount of time until the entry ages out of the cache. For dynamically learned entries only.
<b>Type</b>	Displays IP as the type of entry.
<b>Address</b>	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.

## Syntax

```
show ip cam stack-unit {0-5} [port-set {pipe-number} | {ip-address mask
[longer-prefixes]}| detail | member-info | summary]
```

## Parameters

**0-5** Enter the stack-unit ID from 0 to 5

**pipe-number** Enter the number of the Port-Pipe number. The range is from 0 to 0

<b><i>ip-address mask</i></b> <b>[longer-prefixes]</b>	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keywords <code>longer-prefixes</code> to view routes with a common prefix.
<b>detail</b>	Enter the keyword <code>detail</code> to display the group index ID used by the ecmp routes in the CAM.
<b>member-info</b>	Enter the keywords <code>member-info</code> to display the group index used by the ecmp, the number of egress ports (members) for the ecmp, and the port details of each member.  The detail information under <code>member-info</code> gives the MAC address, VLAN ID, and gateway of every member port of the ecmp.
<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing route prefixes and the total number routes which can be entered in to CAM.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip cam` command shown in the following example.

Field	Description
<b>Destination</b>	Displays the destination route of the index.
<b>EC</b>	Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. For Jumbo line cards, displays 0,1 when ECMP is more than eight.
<b>CG</b>	Displays 0.
<b>V</b>	Displays a 1 if the entry is valid and a 0 otherwise.
<b>C</b>	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
<b>V Id</b>	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
<b>Mac Addr</b>	Displays the next-hop router's MAC address.
<b>Port</b>	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry <code>17cl CP</code> , the CP is the pertinent portion. <ul style="list-style-type: none"> <li>• CP = control processor</li> <li>• Gi = Gigabit Ethernet interface</li> <li>• Te = 10-Gigabit Ethernet interface</li> </ul>

**Example**

```
Dell#show ip cam stack-unit 0 port-set 0 10.10.10.10/32 longer-prefixes
Destination      EC CG V C VId  Mac-Addr          Port
-----
10.10.10.10      0 0 1 1 0    00:00:00:00:00:00  3f01 CP
Dell#
```

**Usage Information**

The following describes the `show ip cam ecmp-group` command shown in the following example.

Field	Description
<b>Prefix Length</b>	Displays the prefix-length or mask for the IP address configured on the linecard 0 port pipe 0.

Field	Description
<b>Current Use</b>	Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port pipe 0.
<b>Initial Size</b>	Displays the CAM size the system allocates for the corresponding mask. The system adjusts the CAM size if the number of routes for the mask exceeds the initial allocation.

### Example (ECMP-Group)

```
Dell#show ip cam stack-unit 0 po 0 ecmp-group detail

Destination EC CG V C VId Mac-Addr          Port ECMP Group-Index
-----
1.1.1.2      0 0 1 0 0 00:01:e8:8a:d6:58 0004 Te 0/3 -
2.1.1.2      0 0 1 0 0 00:01:e8:8a:d6:58 0009 Te 0/8 -
1.1.1.1      0 0 1 1 0 00:00:00:00:00:00 3f01 CP -
2.1.1.1      0 0 1 1 0 00:00:00:00:00:00 3f01 CP -
1.1.1.0      0 0 1 1 0 00:00:00:00:00:00 3f01 CP -
2.1.1.0      0 0 1 1 0 00:00:00:00:00:00 3f01 CP -
100.1.1.    0 1 0 1 0 0 00:01:e8:8a:d6:58 0004 Te 0/3 0
100.1.1.    0 1 0 1 0 0 00:01:e8:8a:d6:58 0009 Te 0/8 0
0.0.0.0     0 0 1 1 0 00:00:00:00:00:00 3f01 CP -
Dell#
```

### Example (Member-Info)

```
Dell#show ip cam stack-unit 0 po 0 ecmp-group member-info detail

Group Index Member Count Mac-Addr          Port Vlan ID Gateway
-----
0          2          00:01:e8:8a:d6:58 Te 0/3 0 1.1.1.2
          00:01:e8:8a:d6:58 Te 0/8 0 2.1.1.2
Dell#
```

## show ip fib stack-unit

View all FIB entries.

**Syntax** `show ip fib stack-unit 0-5 [ip-address [mask] [longer-prefixes] | summary]`

Parameters	Description
<b>0-5</b>	Enter the unit ID, from 0 to 5.
<b>ip-address mask</b>	(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).
<b>longer-prefixes</b>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to view the total number of prefixes in the FIB.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip fib stack-unit` command shown in the following example.

Field	Description
<b>Destination</b>	Lists the destination IP address.
<b>Gateway</b>	Displays either the word "direct" and an interface for a directly connected route or the remote IP address used to forward the traffic.
<b>First-Hop</b>	Displays the first hop IP address.
<b>Mac-Addr</b>	Displays the MAC address.
<b>Port</b>	Displays the egress-port information.
<b>Vld</b>	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
<b>EC</b>	Displays the number of ECMP paths.

### Example

```
Dell#show ip fib stack-unit 0
Destination      Gateway      First-Hop    Mac-Addr      Port Vld EC
-----
10.10.10.10/32  Direct, Nu 0  0.0.0.0  00:00:00:00:00:00  BLK HOLE 0 0
Dell>
```

### Related Commands

[clear ip fib stack-unit](#) — clear FIB entries on a specified stack-unit.

## show ip interface

View IP-related information on all interfaces.

**Syntax** `show ip interface [interface | brief] [configuration]`

Parameters	
<b>interface</b>	(OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For the Management interface, enter the keyword <code>ManagementEthernet</code> followed by zero (0).</li> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> followed by a number. The range is from 1 to 128.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li> <li>For a VLAN, enter the keyword <code>vlan</code> followed by a number from 1 to 4094.</li> </ul>
<b>brief</b>	(OPTIONAL) Enter the keyword <code>brief</code> to view a brief summary of the interfaces and whether an IP address is assigned.
<b>configuration</b>	(OPTIONAL) Enter the keyword <code>configuration</code> to display the physical interfaces with non-default configurations only.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

### Command History

Version	Description
<b>9.11(0.0)</b>	Updated the command output to include the unicast reverse path forwarding (uRPF) status.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following describes the `show ip interface` command shown in the following example.

Lines	Description
<b>TenGigabitEthernet 0/0...</b>	Displays the interface's type, slot/port and physical and line protocol
<b>Internet address...</b>	States whether an IP address is assigned to the interface. If one is, that address is displayed.
<b>IP MTU is...</b>	Displays IP MTU value.
<b>Inbound access...</b>	Displays the name of the any configured incoming access list. If none is configured, the phrase "not set" is displayed.
<b>Proxy ARP...</b>	States whether proxy ARP is enabled on the interface.
<b>Split horizon...</b>	States whether split horizon for RIP is enabled on the interface.
<b>Poison Reverse...</b>	States whether poison for RIP is enabled on the interface
<b>ICMP redirects...</b>	States if ICMP redirects are sent.
<b>ICMP unreachable...</b>	States if ICMP unreachable messages are sent.

### Example

```
Dell#show ip interface tengigabitethernet 0/0
TenGigabitEthernet 0/0 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
IP unicast RPF check is not supported
Dell#
```

### Usage Information

The following describes the `show ip interface brief` command shown in the following example.

Fields	Description
<b>Interface</b>	Displays type of interface and the associated slot and port number.
<b>IP-Address</b>	Displays the IP address for the interface, if configured.
<b>Ok?</b>	Indicates if the hardware is functioning properly.
<b>Method</b>	Displays "Manual" if the configuration is read from the saved configuration.
<b>Status</b>	States whether the interface is enabled (up) or disabled (administratively down).
<b>Protocol</b>	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 0/1 unassigned NO   None   up      down
TenGigabitEthernet 0/2 unassigned YES  None   up      up
TenGigabitEthernet 0/3 unassigned YES  None   up      up
TenGigabitEthernet 0/4 unassigned NO   None   up      down
TenGigabitEthernet 0/5 unassigned NO   None   up      down
TenGigabitEthernet 0/6 unassigned NO   None   up      down
TenGigabitEthernet 0/7 unassigned NO   None   up      down
TenGigabitEthernet 0/8 unassigned NO   None   up      down
TenGigabitEthernet 0/9 unassigned NO   None   up      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 `all` to view all IP addresses assigned to all Management interfaces on the switch.
- connected** (OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
- summary** (OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
- static** (OPTIONAL) Enter the keyword `static` to view non-active routes also.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Example

```
Dell#show ip management-route
Destination      Gateway          State
-----
10.1.2.0/24      ManagementEthernet 0/0  Connected
172.16.1.0/24    10.1.2.4        Active
Dell#
```

# show ip multicast-cam stack-unit

Displays content-addressable memory (CAM) entries.

**Syntax** `show ip multicast-cam stack-unit 0-5 port-set pipe-number [ip-address mask [longer-prefixes] | detail | member-info | summary]`

**Parameters**

- 0-5** Enter the stack-unit ID, from 0 to 5.
- pipe-number** Enter the number of the Port-Pipe number. The range is from 0 to 0.
- ip-address mask [longer-prefix]** (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only.  
Enter the keyword `longer-prefixes` to view routes with a common prefix.
- detail** Enter the keyword `detail` to display the group index ID used by the ecmp routes in the CAM.
- member-info** Enter the keyword `member-info` to display the group index used by the ecmp, the number of egress ports (members) for the ecmp, and the port details of each member. The detail information under `member-info` will give the MAC address, VLAN ID and gateway of every member port of the ecmp.
- summary** (OPTIONAL) Enter the keyword `summary` to view a table listing route prefixes and the total number routes which can be entered in to CAM.



- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information**

The following describes the `show ip fib stack-unit` command shown in the following example.

Field	Description
<b>Destination</b>	Displays the destination route of the index.
<b>CG</b>	Displays 0.
<b>V</b>	Displays a 1 if the entry is valid and a 0 otherwise.
<b>C</b>	Displays the CPU bit.  1 indicates that a packet hitting this entry is forwarded to the control processor, depending on Egress port.
<b>V Id</b>	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
<b>Mac Addr</b>	Displays the next-hop router's MAC address.
<b>Port</b>	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. <ul style="list-style-type: none"> <li>• CP = control processor</li> <li>• Fo= 40 Gigabit Ethernet interface</li> <li>• Te = 10 Gigabit Ethernet interface</li> </ul>

**Example**

```
Dell#show ip multicast-cam stack-unit 0 port-set 0 10.10.10.10/32
longer-prefixes
Destination      EC      CG      V      C      VId      Mac-Addr      Port
-----
10.10.10.10      0       0       0       1       1 0 00:00:00:00:00:00      3f01 CP
Dell#
```

## show ip protocols

View information on all routing protocols enabled and active on the switch.

**Syntax** `show ip protocols`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [hostname | ip-address [mask] [longer-prefixes] | list prefix-list [process-id] | connected | static | summary]`

<b>Parameters</b>	<b><i>ip-address</i></b>	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
	<b><i>mask</i></b>	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
	<b>longer-prefixes</b>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
	<b>list <i>prefix-list</i></b>	(OPTIONAL) Enter the keyword <code>list</code> and the name of a configured prefix list.
	<b><i>process-id</i></b>	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
	<b>connected</b>	(OPTIONAL) Enter the keyword <code>connected</code> to view only the directly connected routes.
	<b>static</b>	(OPTIONAL) Enter the keyword <code>static</code> to view only routes configured by the <code>ip route</code> command.
	<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> .

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** The following describes the `show ip route all` command in the following example.

Field	Description
<b>(undefined)</b>	Identifies the type of route: <ul style="list-style-type: none"> <li>• C = connected</li> <li>• S = static</li> <li>• R = RIP</li> <li>• B = BGP</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• IN = internal BGP</li> <li>• EX = external BGP</li> <li>• LO = Locally Originated</li> <li>• O = OSPF</li> <li>• IA = OSPF inter area</li> <li>• N1 = OSPF NSSA external type 1</li> <li>• N2 = OSPF NSSA external type 2</li> <li>• E1 = OSPF external type 1</li> <li>• E2 = OSPF external type 2</li> <li>• i = IS-IS</li> <li>• L1 = IS-IS level-1</li> <li>• L2 = IS-IS level-2</li> <li>• IA = IS-IS inter-area</li> <li>• * = candidate default</li> <li>• &gt; = non-active route</li> <li>• + = summary routes</li> </ul>
<b>Destination</b>	Identifies the route's destination IP address.
<b>Gateway</b>	Identifies whether the route is directly connected and on which interface the route is configured.
<b>Dist/Metric</b>	Identifies if the route has a specified distance or metric.
<b>Last Change</b>	Identifies when the route was last changed or configured.

### Example

#### Example (Summary)

```
Dell#show ip route summary
Route Source      Active Routes      Non-active Routes
connected         2                   0
static            1                   0
Total             3                   0
Total 3 active route(s) using 612 bytes
Dell#show ip route static ?
|                 Pipe through a command
<cr>
Dell#show ip route static
      Destination      Gateway              Dist/Metric  Last Change
      -----
*sS   0.0.0.0/0          via 10.10.91.9, Te 1/2      1/0         3d2h
Dell#
```

## show ip route list

Display IP routes in an IP prefix list.

<b>Syntax</b>	<code>show ip route list <i>prefix-list</i></code>	
<b>Parameters</b>	<b><i>prefix-list</i></b>	Enter the name of a configured prefix list.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 4/4   120/2        3d0h
R    2.1.1.0/24        via 2.1.4.1, Te 4/4   120/2        3d1h
R    2.1.2.0/24        via 2.1.4.1, Te 4/4   120/1        3d0h
R    2.1.3.0/24        via 2.1.4.1, Te 4/4   120/1        3d1h
C    2.1.4.0/24        Direct, Te 4/4        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 summary`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip route summary` shown in the following example.

Column Heading	Description
<b>Route Source</b>	Identifies how the route is configured in the system.
<b>Active Routes</b>	Identifies the best route if a route is learned from two protocol sources.
<b>Non-active Routes</b>	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.
<b>ospf 100</b>	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
<b>Total 1388 active...</b>	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the the system, this line does not appear.

## Example

```
Dell>show ip route summary

Route Source      Active Routes   Non-active Routes
connected         17              0
static            3              0
ospf 100         1368            2
Intra-area: 762  Inter-area: 1  External-1: 600  External-2: 5
Total            1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Dell>
```

## Related Commands

[show ip route](#) — displays information about the routes found in the switch.

# show ip traffic

View IP, ICMP, UDP, TCP and ARP traffic statistics.

**Syntax** `show ip traffic`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show ip traffic` summary shown in the following example.

Keyword	Definition
<b>unknown protocol...</b>	No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.
<b>not a gateway...</b>	Packets can not be routed; the host/network is unreachable.
<b>security failures...</b>	Counts the number of received unicast/multicast packets that could not be forwarded due to: <ul style="list-style-type: none"><li>route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group</li><li>destination IP address belongs to reserved prefixes; the host/network is unreachable</li></ul>
<b>bad options...</b>	Unrecognized IP option on a received packet.
<b>Frgs:</b>	IP fragments received.
<b>... reassembled</b>	Number of IP fragments that were reassembled.
<b>... timeouts</b>	Number of times a timer expired on a reassembled queue.
<b>... too big</b>	Number of invalid IP fragments received.
<b>... couldn't fragment</b>	Number of packets that could not be fragmented and forwarded.
<b>...encapsulation failed</b>	Counts packets which could not be forwarded due to ARP resolution failure. The system sends an arp request prior to forwarding an IP packet. If a reply is not received, the system repeats the request three times. These packets are counted in encapsulation failed.
<b>Rcvd:</b>	
<b>...short packets</b>	The number of bytes in the packet are too small.

Keyword	Definition
<b>...bad length</b>	The length of the packet was not correct.
<b>...no port broadcasts</b>	The incoming broadcast/multicast packet did not have any listener.
<b>...socket full</b>	The applications buffer is full and the incoming packet are dropped.

The F10 Monitoring MIB provides access to the following statistics.

- **IP Statistics: Bcast: Received:** Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent:** Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received:** Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent:** Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request:** Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies:** Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request:** Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies:** Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy:** Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

### Example

```
Dell#show ip traffic
IP statistics:
  Rcvd: 10021161 total, 3197480 local destination
        2501 format errors, 390 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        115 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
        0 fragmented, 0 couldn't fragment
  Bcast: 6281 received, 0 sent; Mcast: 500 received, 0 sent
  Sent: 6573260 generated, 0 forwarded
        3830 encapsulation failed, 0 no route

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 3 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, 1 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: 2938110 total, 14 checksum errors, 1 no port
        0 short packets, 0 bad length, 1883908 no port broadcasts, 0 socket
  full
  Sent: 329731 total, 1883908 forwarded broadcasts
--More--
```

## show tcp statistics

View information on TCP traffic through the switch.

**Syntax**                show tcp statistics

**Command Modes**    EXEC Privilege

**Supported Modes**   All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## Usage Information

The following describes the `show tcp statistics cp` command shown in the following example.

Field	Description
<b>Rcvd:</b>	Displays the number and types of TCP packets received by the switch. <ul style="list-style-type: none"><li>• Total = total packets received</li><li>• no port = number of packets received with no designated port</li></ul>
<b>0 checksum error...</b>	Displays the number of packets received with the following: <ul style="list-style-type: none"><li>• checksum errors</li><li>• bad offset to data</li><li>• too short</li></ul>
<b>329 packets...</b>	Displays the number of packets and bytes received in sequence.
<b>17 dup...</b>	Displays the number of duplicate packets and bytes received.
<b>0 partially...</b>	Displays the number of partially duplicated packets and bytes received.
<b>7 out-of-order...</b>	Displays the number of packets and bytes received out of order.
<b>0 packets with data after window</b>	Displays the number of packets and bytes received that exceed the switch's window size.
<b>0 packets after close</b>	Displays the number of packet received after the TCP connection was closed.
<b>0 window probe packets...</b>	Displays the number of window probe and update packets received.
<b>41 dup ack...</b>	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
<b>10184 ack...</b>	Displays the number of acknowledgement packets and bytes received.
<b>Sent:</b>	Displays the total number of TCP packets sent and the number of urgent packets sent.
<b>25 control packets...</b>	Displays the number of control packets sent and the number retransmitted.
<b>11603 data packets...</b>	Displays the number of data packets sent.
<b>24 data packets retransmitted</b>	Displays the number of data packets resent.
<b>355 ack..</b>	Displays the number of acknowledgement packets sent and the number of packet delayed.
<b>0 window probe...</b>	Displays the number of window probe and update packets sent.
<b>7 Connections initiated...</b>	Displays the number of TCP connections initiated, accepted, and established.
<b>14 Connections closed...</b>	Displays the number of TCP connections closed, dropped.
<b>20 Total rxmt...</b>	Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.
<b>0 Keepalive....</b>	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

## Example

```
Dell#show tcp statistics

Rcvd: 9849 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
5735 packets (7919 bytes) in sequence
20 dup packets (2 bytes)
```

```
0 partially dup packets (0 bytes)
1 out-of-order packets (0 bytes)
0 packets ( 0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
0 dup ack packets, 0 ack packets with unsend data
6671 ack packets (152813 bytes)
Sent: 6778 Total, 0 urgent packets
7 control packets
6674 data packets (152822 bytes)
12 data packets (1222 bytes) retransmitted
85 ack only packets (5677 delayed)
0 window probe packets, 0 window update packets
0 Connections initiated, 7 connections accepted, 7 connections
established
8 Connections closed (including 4 dropped, 0 embryonic dropped)
12 Total rxmt timeout, 1 connections dropped in rxmt timeout
26 Keepalive timeout, 25 keepalive probe, 1 Connections dropped in
keepalive
Dell#
```



# Internet Protocol Security (IPSec)

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — Connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — Confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — Algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes: Transport and Tunnel.

- Transport is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- Tunnel mode is used to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating virtual private networks (VPNs).

Transport mode provides IP packet payload protection using ESP. You can use ESP alone or in combination with AH to provide additional authentication. AH protects data from modification but does not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. The SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.

## NOTE:

The Dell EMC Networking OS supports IPSec only for FTP and telnet protocols (ports 20, 21, and 23). The system rejects if you configure IPSec for other protocols.

## Topics:

- [crypto ipsec transform-set](#)
- [crypto ipsec policy](#)
- [management crypto-policy](#)
- [match](#)
- [session-key](#)
- [show crypto ipsec transform-set](#)
- [show crypto ipsec policy](#)
- [transform-set](#)

## crypto ipsec transform-set

Create a transform set, or combination of security algorithms and protocols, of cryptos.

### Syntax

```
crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-
authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}
```

To delete a transform set, use the `no crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}` command.

### Parameters

<b><i>name</i></b>	Enter the name for the transform set.
<b>ah-authentication</b>	Enter the keywords <code>ah-authentication</code> then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic. <ul style="list-style-type: none"> <li>• <code>md5</code> — Use Message Digest 5 (MD5) authentication.</li> <li>• <code>sha1</code> — Use Secure Hash Algorithm 1 (SHA-1) authentication.</li> </ul>

- null — Causes an encryption policy configured for the area to not be inherited on the interface.

**esp-authentication**

Enter the keywords `esp-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.

- md5 — Use Message Digest 5 (MD5) authentication.
- sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication.
- null — Causes an encryption policy configured for the area to not be inherited on the interface.

**esp-encryption**

Enter the keywords `esp-encryption` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.

- 3des — Use 3DES encryption.
- cbc — Use CDC encryption.
- des — Use DES encryption.
- null — Causes an encryption policy configured for the area to not be inherited on the interface.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- Both sides of the link must specify the same transform set.
- You can create up to 64 transform sets.

**Example**

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

## crypto ipsec policy

Create a crypto policy used by ipsec.

**Syntax** `crypto ipsec policy name seq-num ipsec-manual`

To delete a crypto policy entry, use the `no crypto ipsec policy name seq-num ipsec-manual` command.

**Parameters**

- name** Enter the name for the crypto policy set.
- seq-num** Enter the sequence number assigned to the crypto policy entry.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This command creates a crypto policy entry and enters the crypto policy configuration mode for configuring the flow parameters.

**Example**

```
Dell(conf)#crypto ipsec policy West 10 ipsec-manual
Dell(conf-crypto-policy)#
```

## management crypto-policy

Apply the crypto policy to management traffic.

**Syntax** `management crypto-policy name`

To remove the management traffic crypto policy, use the `no management crypto-policy name` command.

**Parameters** *name* Enter the name for the crypto policy.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## match

Match a sequence number to the transmission control protocol (TCP)/user datagram protocol (UDP) packets.

**Syntax** `match seq-num {tcp | udp} {ipv6 | ip} port-num dest-ip dest-port-num`

To remove the match filter for the crypto map, use the `no match seq-num` command.

**Parameters**

- seq-num* Enter the match command sequence number. The range is from 0 to 255.
- tcp* Enter the keyword `tcp` to configure a TCP access list filter.
- udp* Enter the keyword `udp` to configure a UDP access list filter.
- ipv6* Enter the source IPv6 address.
- ip* Enter the source IPv4 address.
- port-num* Enter the source port number. The range is from 0 to 65535
- dest-ip* Enter the destination IP address.
- dest-port-num* Enter the destination port number. The range is from 0 to 65535.

**Defaults** none

**Command Modes** CONFIG-CRYPTO-POLICY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

UDP is not supported. Only TCP 23 telnet and 21 FTP are supported.

## Example

```
Dell(conf-crypto-policy)#match 0 tcp a::1 /128 0 a::2 /128 23
Dell(conf-crypto-policy)#match 1 tcp a::1 /128 23 a::2 /128 0
Dell(conf-crypto-policy)#match 2 tcp a::1 /128 0 a::2 /128 21
Dell(conf-crypto-policy)#match 3 tcp a::1 /128 21 a::2 /128 0
Dell(conf-crypto-policy)#match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32 23
Dell(conf-crypto-policy)#match 5 tcp 1.1.1.1 /32 23 1.1.1.2 /32 0
Dell(conf-crypto-policy)#match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32 21
Dell(conf-crypto-policy)#match 7 tcp 1.1.1.1 /32 21 1.1.1.2 /32 0
```

# session-key

Specify the session keys used in the crypto policy entry.

**Syntax** `session-key {inbound | outbound} {ah spi hex-key-string | esp spi encrypt hex-key-string auth hex-key-string}`

To delete the session key information from the crypto policy, use the `no session-key {inbound | outbound} {ah | esp}` command.

## Parameters

<b>name</b>	Enter the name of the host to delete. Enter * to delete all host table entries.
<b>inbound</b>	Specify the inbound session key for IPsec.
<b>outbound</b>	Specify the outbound session key for IPsec.
<b>ah</b>	Use the AH protocol when you select the AH transform set in the crypto policy.
<b>esp</b>	Use the ESP protocol when you select the ESP transform set in the crypto policy.
<b>spi</b>	Enter the security parameter index number.
<b>hex-key-string</b>	Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.
<b>encrypt</b>	Indicates the ESP encryption transform set key string.
<b>auth</b>	Indicates the ESP authentication transform set key string.

**Defaults** none

**Command Modes** CONF-CRYPTO-POLICY

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

- This command is only available in the ipsec-manual model.
- The key information entry is associated with the global method for enabling clear text or encrypted display in the running config.

# show crypto ipsec transform-set

Display the transform set configuration.

**Syntax** `show crypto ipsec transform-set name`

**Parameters** **name** Enter the name of the transform set.

**Command Modes** EXEC

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.2)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf)#do show crypto ipsec transform-set
Transform-Set Name      : ts1
Transform-Set refCnt   : 0
AH Transform           : md5
ESP Auth Transform     :
ESP Encry Transform    :
Dell(conf)#
```

## show crypto ipsec policy

Display the crypto policy configuration.

**Syntax** show crypto ipsec policy *name*

**Parameters** *name* Enter the name for the crypto policy set.

**Command Modes** EXEC

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-crypto-policy)#do show crypto ipsec policy

Policy name           : poll
Policy refcount       : 0
Sequence Num         : 1
SA Mode               : IPSEC-MANUAL
Transform-Set Name    :
Peer IP Address       :
Inbound AH SPI        : 0
Inbound ESP Auth SPI : 0
Inbound ESP Encry SPI : 0
Inbound AH Key        : [0]::
Inbound ESP Auth Key  : [0]::
Inbound ESP Encry Key : [0]::
Outbound AH SPI       : 0
Outbound ESP Auth SPI : 0
Outbound ESP Encry SPI : 0
Outbound AH Key       : [0]::
Outbound ESP Auth Key : [0]::
Outbound ESP Encry Key : [0]::

Match sequence Num   : 2
Protocol type        : tcp
IP or IPv6           : IP
Source address       : 1.1.1.1
Source mask          : /32
Source port          : 0
Destination address  : 1.1.1.2
Destination mask     : /32
Destination port     : 23
```

```
source-interface name :
source-interface num  :

Dell(conf-crypto-policy)#
```

## transform-set

Specify the transform set the crypto policy uses.

<b>Syntax</b>	<code>transform-set <i>transform-set-name</i></code>						
	To delete a transform set from the crypto policy, use the <code>no transform-set <i>transform-set-name</i></code> command.						
<b>Parameters</b>	<b><i>transform-set-name</i></b> Enter the name for the crypto policy transform set.						
<b>Defaults</b>	none						
<b>Command Modes</b>	CONFIG-CRYPTO-POLICY						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

# IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking switch.

**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 \(Configuration\)](#) command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.

### Topics:

- [IPv6 ACL Commands](#)

## IPv6 ACL Commands

The following commands configure IPv6 ACLs.

### 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**

<b>default</b>	Use the default CAM profile settings, and set the CAM as follows: <ul style="list-style-type: none"> <li>• L3 ACL (ipv4acl): <b>6</b></li> <li>• L2 ACL(l2acl): <b>5</b></li> <li>• IPv6 L3 ACL (ipv6acl): <b>0</b></li> <li>• L3 QoS (ipv4qos): <b>1</b></li> <li>• L2 QoS (l2qos): <b>1</b></li> </ul>
<b>l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10</b>	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 <code>ipv6acl</code> range must be a factor of 2.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>For the new settings to take effect, save the new CAM settings to the startup-config (<code>write mem</code> or <code>copy run start</code>), then reload the system.</p> <p>The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.</p> <p>When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.</p> <p>Ranges for the CAM profiles are from 1 to 10, except for the <code>ipv6acl</code> profile which is from 0 to 10. The <code>ipv6acl</code> allocation must be a factor of 2 (2, 4, 6, 8, 10).</p>	

## cam-acl-egress

Allocate space for IPv6 egress ACLs.

<b>Syntax</b>	<code>cam-acl-egress {default   l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}</code>	
<b>Parameters</b>	<b>default</b>	Use the default CAM profile settings, and set the CAM as follows: <ul style="list-style-type: none"> <li>• L2 ACL(l2acl): <b>1</b></li> <li>• L3 ACL (ipv4acl): <b>1</b></li> <li>• IPv6 L3 ACL (ipv6acl): <b>2</b></li> </ul>
	<b>l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4</b>	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 <code>ipv6acl</code> range must be a factor of 2.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	<p>For the new settings to take effect, save the new CAM settings to the startup-config (<code>write mem</code> or <code>copy run start</code>), then reload the system.</p> <p>The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated.</p> <p>When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.</p> <p>Ranges for the CAM profiles are from 1 to 10, except for the <code>ipv6acl</code> profile which is from 0 to 10. The <code>ipv6acl</code> allocation must be a factor of 2 (2, 4, 6, 8, 10).</p>	
--------------------------	---	--

### 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
```

## 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**

- access-list-name*** Enter the access list name as a string, up to 140 characters.
- cpu-qos** Enter the keyword `cpu-qos` to assign this ACL to control plane traffic only (CoPP).
- permit** Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
- deny** Enter the keyword `deny` 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for CoPP for OSPFv3 on the MXL 10/40GbE Switch IO Module.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 that existed in Dell Networking OS releases 9.3(0.0) and earlier

**Related Commands** [show config](#) — views the current configuration.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# 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} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

<b>Parameters</b>	<b><i>ip-protocol-number</i></b>	Enter an IPv6 protocol number. The range is from 0 to 255.
	<b>icmp</b>	Enter the keyword <code>icmp</code> to filter internet Control Message Protocol version 6.
	<b>ipv6</b>	Enter the keyword <code>ipv6</code> to filter any internet Protocol version 6.
	<b>tcp</b>	Enter the keyword <code>tcp</code> to filter the Transmission Control protocol.
	<b>udp</b>	Enter the keyword <code>udp</code> to filter the User Datagram Protocol.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
	<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
	<b>dscp</b>	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
	<b>order</b>	(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 ( <b>255</b> ).
	<b>fragments</b>	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
	<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	<b>threshold-in-<i>msgs</i></b>	(OPTIONAL) Enter the <code>threshold-in-<i>msgs</i></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.
	<b>interval <i>minutes</i></b>	(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.
	<b>monitor</b>	(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** Not configured.

**Command Modes** ACCESS-LIST

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
	<b>9.3(0.0)</b>	Added support for logging of ACLs on the MXL 10/40GbE Switch IO Module.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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} [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.

<b>Parameters</b>	<b>source address</b>	Enter the IPv6 address of the network or host from which the packets were sent in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
	<b>mask</b>	Enter a network mask in /prefix format (/x).
	<b>any</b>	Enter the keyword <code>any</code> to specify that all routes are subject to the filter.
	<b>host ipv6-address</b>	Enter the keyword <code>host</code> then the IPv6 address of the host in the x:x:x:x format. The :: notation specifies successive hexadecimal fields of zero.
	<b>destination address</b>	Enter the IPv6 address of the network or host to which the packets are sent in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128. The :: notation specifies successive hexadecimal fields of zero.
	<b>message-type</b>	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
	<b>byte</b>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
	<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	<b>threshold-in-msgs count</b>	(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.
	<b>interval minutes</b>	(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.
	<b>monitor</b>	(OPTIONAL) Enter the keyword <code>monitor</code> to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

**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

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added the support for flow-based monitoring on the MXL 10/40GbE Switch IO Module platform
9.3(0.0)	Added the support for logging of ACLs on the MXL 10/40GbE Switch IO Module platform
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

## 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).

## show cam-acl

Show space allocated for IPv6 ACLs.

**Syntax** `show cam-acl`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 0 --
          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#

```

**Related Commands** [cam-acl](#) — configures CAM profiles to support IPv6 ACLs.

## show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

**Syntax** `show cam-acl-egress`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```

Dell#show cam-acl-egress

-- Chassis Egress Cam ACL --
      Current Settings(in block sizes)
      1 block = 256 entries
L2Acl      :      1
Ipv4Acl    :      1
Ipv6Acl    :      2

-- stack-unit 0 --
      Current Settings(in block sizes)
L2Acl      :      1
Ipv4Acl    :      1
Ipv6Acl    :      2

```

**Related Commands** [cam-acl](#) — configures CAM profiles to support IPv6 ACLs.

## IPv6 Basics

This chapter describes IPv6 basic commands.

### Topics:

- `clear ipv6 fib`
- `clear ipv6 route`
- `clear ipv6 mld_host`
- `ipv6 address autoconfig`
- `ipv6 address`
- `ipv6 address eui64`
- `ipv6 control-plane icmp error-rate-limit`
- `ipv6 flowlabel-zero`
- `ipv6 host`
- `ipv6 name-server`
- `ipv6 nd dad attempts`
- `ipv6 nd disable-reachable-timer`
- `ipv6 nd dns-server`
- `ipv6 nd prefix`
- `ipv6 nd reachable-time`
- `ipv6 route`
- `ipv6 unicast-routing`
- `show ipv6 cam stack-unit`
- `show ipv6 control-plane icmp`
- `show ipv6 fib stack-unit`
- `show ipv6 flowlabel-zero`
- `show ipv6 interface`
- `show ipv6 mld_host`
- `show ipv6 route`
- `trust ipv6-diffserv`

## clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a linecard or stack unit.

**Syntax** `clear ipv6 fib linecard slot | stack-unit unit-number`

**Parameters**

<b><i>slot</i></b>	Enter the slot number to clear the FIB for a linecard.
<b><i>unit-number</i></b>	Enter the stack member number.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

**Syntax** `clear ipv6 route {* | ipv6-address prefix-length}`

**Parameters**

- \*** Enter the \* to clear (refresh) all routes from the IPv6 routing table.
- ipv6-address prefix-length** Enter the IPv6 address in the x:x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128.

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# clear ipv6 mld\_host

Clear the IPv6 MLD host counters and reset the elapsed time.

**Syntax** `clear ipv6 mld_host`

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ipv6 address autoconfig

Configure IPv6 address auto-configuration for the management interface.

**Syntax** `ipv6 address autoconfig`

To disable the address autoconfig operation on the management interface, use the `no ipv6 address autoconfig` command.

**Default** Disabled

**Command Modes** INTERFACE (management interface only)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- SAA can configure up to two addresses. If any preferred prefix or valid timers time out, the corresponding address are deprecated or removed. If an address is removed due to a time-out, an

address from the current unused prefix is used to create a new address. If there are no remaining prefixes, the software waits to receive a new prefix from the RA.


- If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. Manual and auto-configurations are not supported on a single management interface.
- Removing auto-configuration removes all auto-configured IPv6 addresses and the link-local IPv6 address from that management interface.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across a platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

## ipv6 address

Configure an IPv6 address to an interface.

**Syntax** `ipv6 address {ipv6-address prefix-length}`  
To remove the IPv6 address, use the `no ipv6 address {ipv6-address prefix-length}` command.

**Parameters** *ipv6-address* 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.

**Defaults** none

**Command Modes** INTERFACE


**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the “no” form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

 **NOTE:** Do not use the /128 prefix length on physical or port channel interfaces. You can use the /128 prefix length on loopback interfaces.

**Example**

```
Dell(conf)#interface tengigabitethernet x/x
Dell(conf-if-te-x/x)#ipv6 address ?
X:X:X:X::X IPv6 address
Dell(conf-if-te-x/x)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
Dell(conf-if-te-x/x)#ipv6 address 2002:1:2::3 /96 ?
```



```
Dell (conf-if-te-x/x)#ipv6 address 2002:1:2::3 /96
Dell (conf-if-te-x/x)#show config
```

## ipv6 address eui64


Configure IPv6 EUI64 address configuration on the interface.

**Syntax** `ipv6 address {ipv6-address prefix-length} eui64`

To disable IPv6 EUI64 address autoconfiguration, use the `no ipv6 address {ipv6-address prefix-length} eui64` command.

**Parameters**

<b><i>ipv6-address</i></b>	Enter the IPv6 prefix in the x:x:x::x format then the prefix length in the /x format.
<b><i>prefix-length</i></b>	The range is from /0 to /128.

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

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command allows you to create an EUI64 address based on the specified prefix and MAC address only. Prefixes may be configured on the interface using the `ipv6 nd prefix` command without creating an EUI64 address.

### Example

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

## ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets per second that can be sent per second.

**Syntax** `ipv6 control-plane icmp error-rate-limit {1-200}`

To restore the default value, use the `no ipv6 control-plane icmp error-rate-limit` command.

**Parameters**

<b>pps</b>	Enter the maximum number of error packets generated per second. The range is from 1 to 200, where 0 disables the rate-limiting.
------------	---

**Default** 100 pps

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

**Syntax** `ipv6 flowlabel-zero`  
To disable the 0 from being set in the field and allow the rotocol operations to fill the field, use the `no ipv6 flowlabel-zero` command.

**Default** Disabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, set the new flowlabel to zero.

# ipv6 host

Assign a name and IPv6 address the host-to-IPv6 address mapping table uses.

**Syntax** `ipv6 host name ipv6-address`  
To remove an IP host, use the `no ipv6 host name {ipv6-address}`.

**Parameters**

- name** Enter a text string to associate with one IP address.
- ipv6-address** Enter the IPv6 address (X:X:X:X) to be mapped to the name.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

**Syntax** `ipv6 name-server ipv6-address [ipv6-address2... ipv6-address6]`  
To remove a name server, use the `no ipv6 name-server ipv6-address` command.

**Parameters**

- ipv6-address** Enter the IPv6 address (X:X:X:X) of the name server to be used.  
 **NOTE:** The :: notation specifics successive hexadecimal fields of zeros.
- ipv6-address2... ipv6-address6** (OPTIONAL) Enter up to five more IPv6 addresses, in the x:x:x:x format, of name servers to be used. Separate the IPv6 addresses with a space.

**Defaults** none  
**Command Modes** CONFIGURATION  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can separately configure both IPv4 and IPv6 domain name servers.

## ipv6 nd dad attempts

To perform duplicate address detection (DAD) on the management interface, configure the number of neighbor solicitation messages that are sent.

**Syntax** `ipv6 nd dad attempts {number of attempts}`  
To restore the default value, use the `no ipv6 nd dad attempts` command.

**Parameters** *number of attempts* Enter the number of attempts to be made to detect a duplicate address. The range is from 0 to 15. Setting the value to 0 disables DAD on the interface.

**Default** 3 attempts

**Command Modes** INTERFACE (management interface only)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 nd disable-reachable-timer

Keep the learnt neighbor discovery entries stateless so that the entries do not time out.

**Syntax** `ipv6 nd disable-reachable-timer`  
To restore to default, use the `no ipv6 nd disable-reachable-timer` command.

**Default** Disabled

**Command Modes** INTERFACE

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

Version	Description
<b>9.11.0.1</b>	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S4810, S4820, S5000, S6000, S6010-ON, S6000-ON, S6100-ON, Z9100-ON, C9010, Z9500, MXL, and FN IOM.

# ipv6 nd dns-server

Configures Recursive DNS Server (RDNSS) addresses to be distributed via IPv6 router advertisements to an IPv6 device.

<b>Syntax</b>	<code>ipv6 nd dns-server {<i>ipv6-RDNSS-address</i>} {<i>lifetime</i>   <i>infinite</i>}</code> To remove the IPv6 RDSS configuration, use <code>no ipv6 nd dns-server {<i>ipv6-RDNSS-address</i>} {<i>lifetime</i>   <i>infinite</i>}</code>	
<b>Parameters</b>	<b><i>ipv6-RDNSS-address</i></b>	Enter the IPv6 Recursive DNS Server's (RDNSS) address. You can specify up to 4 IPv6 RDNSS server addresses.
	<b><i>lifetime</i></b>	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 <i>infinite</i> , 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 <i>lifetime</i> or <i>infinite</i> parameter.
	<b><i>infinite</i></b>	Enter the keyword <i>infinite</i> to specify that the RDNSS lifetime does not expire.
<b>Defaults</b>	Not Configured	
<b>Command Modes</b>	INTERFACE CONFIG	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced on the MXL.
<b>Usage Information</b>	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 <i>lifetime</i> or <i>infinite</i> parameter.	
<b>Example</b>		

# ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

<b>Syntax</b>	<code>ipv6 nd prefix {<i>ipv6-prefix</i>   <i>prefix-length</i>   <i>default</i>} [<i>no-advertise</i>]   [<i>no-autoconfig</i>] [<i>no-rtr-address</i>] [<i>off-link</i>] [<i>lifetime</i> {<i>valid</i>   <i>infinite</i>}] {<i>preferred</i>   <i>infinite</i>}}</code>	
<b>Parameters</b>	<b><i>ipv6-prefix</i></b>	Enter an IPv6 prefix.
	<b><i>prefix-length</i></b>	Enter the prefix then the prefix length. The length range is from 0 to 128.
	<b><i>default</i></b>	Enter the keyword <i>default</i> to set default parameters for all prefixes.
	<b><i>no-advertise</i></b>	Enter the keyword <i>no-advertise</i> to prevent the specified prefix from being advertised.
	<b><i>no-autoconfig</i></b>	Enter the keywords <i>no-autoconfig</i> to disable Stateless Address Autoconfiguration.
	<b><i>no-rtr-address</i></b>	Enter the keyword <i>no-rtr-address</i> to exclude the full router address from router advertisements (the R bit is not set).
	<b><i>off-link</i></b>	Enter the keywords <i>off-link</i> to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
	<b><i>valid-lifetime</i>   <i>infinite</i></b>	Enter the amount of time that the prefix is advertised, or enter <i>infinite</i> for an unlimited amount of time. The range is from 0 to 4294967295. The default is

**2592000**. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.

**preferred-lifetime | infinite**

Enter the amount of time that the prefix is preferred, or enter *infinite* for an unlimited amount of time. The range is from 0 to 4294967295. The default is **2592000**. The maximum value means that the preferred lifetime and does not expire.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the *default* keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the *ipv6 nd prefix default no-autoconfig* command.

## ipv6 nd reachable-time

Configure the amount of time before an IPv6 neighbor is considered unreachable.

**Syntax** `ipv6 nd reachable-time reachable-time`

To restore to default, use the `no ipv6 nd reachable-time` command.

**Parameters**

**reachable-time**

Enter the reachable time in milliseconds. The value is from 0 to 3600000. The default value is 0.

**Default** Disabled

**Command Modes** INTERFACE

**Command History**

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

**Version**

**Description**

**9.12(1.0)**

Introduced on the S5048F-ON.

**Legacy version**

Introduced on the S series and Z series.

## ipv6 route

Establish a static IPv6 route.


**Syntax** `ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]`

To remove the IPv6 route, use the `no ipv6 route ipv6-address prefix-length {ipv6-address | interface | interface ipv6-address} [distance] [tag value] [permanent]` command.

**Parameters**


**ipv6-address  
prefix-length**

Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

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

- interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
- For a loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383.
  - For the null interface, enter the keyword `null` then zero (0).
  - For a port channel interface, enter the keyword `port-channel` then the port channel number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
  - For a VLAN interface, enter the keyword `VLAN` then the vlan number. The range is from 1 to 4094.


If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.

**ipv6-address** (OPTIONAL) Enter the forwarding router IPv6 address in the `x:x:x:x` format.  
 **NOTE:** The `::` notation specifies successive hexadecimal fields of zeros.

**distance** (OPTIONAL) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.

**tag value** (OPTIONAL) Enter the keyword `tag` then a tag value number. The range is from 1 to 4294967295.

**permanent** (OPTIONAL) Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down.

 **NOTE:** If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.

**Defaults** none  
**Command Modes** CONFIGURATION  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When the interface goes down, the system withdraws the route. The route is re-installed by the system when the interface comes back up. When a recursive resolution is “broken,” the system withdraws the route. The route is re-installed by the system 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.

**Example**

```
Dell(conf)#ipv6 route ?
X:X:X:X::X          IPv6 prefix x:x:y
Dell(conf)#ipv6 route 44::0 ?
/nn                /nn Mask in slash format
Dell(conf)#ipv6 route 44::0 /64 ?
X:X:X:X::X        Forwarding router's address
gigabitethernet   Gigabit Ethernet interface
loopback          Loopback interface
null              Null interface
port-channel      Port-Channel interface
tenGigabitethernet TenGigabit Ethernet interface
fortyGigE         FortyGigabit Ethernet interface
tunnel            Tunnel interface
vlan              Vlan interface
```

```

Dell(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>                Distance metric for this route
permanent              Permanent route
tag                    Set tag for this route

Dell(conf)#ipv6 route 44::0 /64 33::1
Dell(conf)#ipv6 route 44::0 /64 tengigabitethernet 0/1 ?
X:X:X:X:X             Forwarding router's address
Dell(conf)#ipv6 route 44::0 /64 tengigabitethernet 0/1 66::1
Dell(conf)#

```

**Related Commands** [show ipv6 route](#) — views the IPv6 configured routes.

## ipv6 unicast-routing

Enable IPv6 Unicast routing.

**Syntax** `ipv6 unicast-routing`  
 To disable unicast routing, use the `no ipv6 unicast-routing` command.

**Defaults** Enabled

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Because this command is enabled by default, it does not appear in the running configuration. When you disable unicast routing, the `no ipv6 unicast-routing` command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, the system generates a syslog message indicating the action.

Disabling unicast routing on a chassis causes the following behavior:

- static and protocol learned routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router `bgp`) is deleted
- IPv6 Multicast traffic continues to flow unhindered

## show ipv6 cam stack-unit

Displays the IPv6 CAM entries for the specified stack-unit.


**Syntax** `show ipv6 cam stack-unit unit-number port-set {0-0} [summary | index | ipv6 address]`

**Parameters**

- unit-number** Enter the stack unit's ID number. The range is from 0 to 5.
- port-set** Enter the keyword `Port Set`.
- summary** (OPTIONAL) Enter the keyword `summary` to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.

**index** (OPTIONAL) Enter the index in the IPv6 CAM.

**ipv6-address** Enter the IPv6 address in the x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.

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

**Defaults** none


**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

 **NOTE:** If a route has a mask greater than 64, no output is displayed for `show ipv6 cam stack-unit unit-number port-set {0-1} ipv6-address`, but an equivalent /64 entry would be listed in the `show ipv6 cam stack-unit unit-number port-set {0-0}` output. Similarly, if there is more than one ECMP object with a destination route that has a mask greater than 64, if the first 64 bits in the destination routes of the ECMP objects are the same, only one route is installed in CAM even though multiple ECMP path entries exist.

## show ipv6 control-plane icmp

Displays the status of the icmp control-plane setting for the error eate limit setting.

**Syntax** `show ipv6 control-plane icmp`

**Default** 100

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [ipv6 flowlabel-zero](#) — Configure IPv6 address auto-configuration for the management interface.

## show ipv6 fib stack-unit

View all FIB entries.

**Syntax** `show ipv6 fib stack-unit unit-number [summary | ipv6-address]`


**Parameters**

**slot-number** Enter the number of the stack unit. The range is from 0 to 5.

**summary** (OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.

**ipv6-address** Enter the IPv6 address in the x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128.



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

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Host tables are not stored in CAM tables. Entries for `camIndex` displays as zero (0) on the `show ipv6 fib stack-unit` output for neighbor entries, such as address resolution protocol (ARP) entries.

## show ipv6 flowlabel-zero

Display the flow label zero setting.

**Syntax** `show ipv6 flowlabel-zero`

**Default** Disabled

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [ipv6 nd dad attempts](#) — Configure system to set the flow label field in the packets to zero.

## show ipv6 interface

Display the status of interfaces configured for IPv6.

**Syntax** `show ipv6 interface interface [brief] [configured] [gigabitethernet slot | slot/port] [linecard slot-number] [loopback interface-number] [managementethernet slot/port] [port-channel number] [tengigabitethernet slot | slot/port] [fortyGigE slot | slot/port] [vlan vlan-id]`

Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information:
		<ul style="list-style-type: none"><li>• For a Loopback interface, enter the keyword <code>Loopback</code> then a number from 0 to 16383.</li><li>• For the Null interface, enter the keyword <code>null</code> then zero (0).</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For stacking, enter the keywords <code>stack-unit</code> then the stack-unit ID.</li><li>• For a tunnel interface, enter the keyword <code>tunnel</code> then the tunnel ID.</li><li>• For a VLAN interface, enter the keyword <code>VLAN</code>.</li><li>• For a port channel interface, enter the keywords <code>port-channel</code>.</li></ul>
	<b>brief</b>	(OPTIONAL) View a summary of IPv6 interfaces.
	<b>configured</b>	(OPTIONAL) View information on all IPv6 configured interfaces.

<b>gigabitethernet</b>	(OPTIONAL) View information for an IPv6 gigabitethernet interface.
<b>linecard slot/ port</b>	(OPTIONAL) View information for a specific IPv6 linecard or stack-unit. The range is 0 to 11.
<b>managementethernet slot/port</b>	(OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).
<b>loopback</b>	(OPTIONAL) View information for IPv6 Loopback interfaces.
<b>port-channel</b>	(OPTIONAL) View information for IPv6 port channels.
<b>tengigabitethernet</b>	(OPTIONAL) View information for an IPv6 tengigabitethernet interface.
<b>fortyGigE</b>	(OPTIONAL) View information for an IPv6 fortygigabitethernet interface.
<b>vlan</b>	(OPTIONAL) View information for IPv6 VLANs.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.11(0.0)</b>	Updated the command output to include the unicast reverse path forwarding (uRPF) status.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The Management port is enabled by default (`no shutdown`). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

**Example**

```
Dell#show ipv6 interface tengigabitethernet 0/2
TenGigabitEthernet 0/2 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fea7:497e
  Global Unicast address(es):
    100::2, subnet is 100::/64 (MANUAL)
    Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:2
    ff02::1:ffa7:497e
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 39610 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 198 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
  IPv6 unicast RPF check is not supported
Dell#
```

**Example (Managementethernet)**

```
Dell#show ipv6 interface managementethernet 0/0
ManagementEthernet 0/0 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fea7:497e
  Global Unicast address(es):
```

```

    Actual address is 300::1, subnet is 300::/64 (MANUAL)
    Remaining lifetime: infinite
    Virtual-IP IPv6 address is not set
Global Anycast address(es):
Joined Group address(es):
    ff02::1
    ff02::1:ff00:1
    ff02::1:ffa7:497e
ND MTU is 0
ICMP redirects are not sent
DAD is enabled, number of DAD attempts: 3
ND reachable time is 20410 milliseconds
ND base reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
ND hop limit is 64
Dell#

```

#### Example (Brief)

```

Dell#show ipv6 interface brief
TenGigabitEthernet 0/2          [administratively down/down]
    fe80::201:e8ff:fea7:497e
    2002:1:2::3/96
TenGigabitEthernet 0/8          [up/up]
    fe80::201:e8ff:fea7:497e
    100::2/64
ManagementEthernet 0/0         [up/up]
    fe80::201:e8ff:fea7:497e
    300::1/64
Dell#

```

#### Example (tunnel)

```

Dell#show ipv6 interface tun 1
Tunnel 1 is up, line protocol is up
IPV6 is enabled
Link Local address: fe80::201:e8ff:fea7:497e
Global Unicast address(es):
    400::1, subnet is 400::/64 (MANUAL)
    Remaining lifetime: infinite
Global Anycast address(es):
Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:1
    ff02::1:ffa7:497e
ND MTU is 0
ICMP redirects are not sent
DAD is enabled, number of DAD attempts: 3
ND reachable time is 20410 milliseconds
ND base reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 198 to 600 seconds
ND router advertisements live for 1800 seconds
ND advertised hop limit is 64
IPv6 hop limit for originated packets is 64
IPv6 unicast RPF check is not supported
Dell#

```

## show ipv6 mld\_host

Display the IPv6 MLD host counters.

**Syntax**                show ipv6 mld\_host

**Command Modes** EXEC

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show ipv6 mld-host` command shown in the following example.

Field	Description
<b>Valid MLD Packets</b>	The total number of packets received and sent from the last time the elapsed time was cleared.
<b>Reports</b>	The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.
<b>Leaves</b>	The number of Multicast leaves that have been sent.
<b>MLDv1 queries</b>	The number of MLDv1 queries that have been received.
<b>MLDv2 queries</b>	The number of MLDv2 queries that have been received.
<b>Malformed Packets</b>	The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

## Example

```
MLD Host Traffic Counters
Elapsed time since counters cleared: 0028:33:52
      Received      Sent
Valid MLD Packets  97962      18036
Reports           79962      18034
Leaves            -----      0
MLDv2 Queries     18000      -----
MLDv1 Queries     0          -----
Errors:
Malformed Packets: 4510
```


# show ipv6 route

Displays the IPv6 routes.

## Syntax

```
show ipv6 route [ipv6-address prefix-length] [hostname] [all] [bgp as
number] [connected] [isis tag] [list prefix-list name] [ospf process-id]
[rip] [static] [summary]
```

## Parameters

<b>ipv6-address</b>	(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.
<b>prefix-length</b>	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>hostname</b>	(OPTIONAL) View information for this IPv6 routes with Host Name.
<b>all</b>	(OPTIONAL) View information for all IPv6 routes.
<b>bgp</b>	(OPTIONAL) View information for all IPv6 BGP routes.
<b>connected</b>	(OPTIONAL) View only the directly connected IPv6 routes.
<b>isis</b>	(OPTIONAL) View information for all IPv6 IS-IS routes.
<b>list</b>	(OPTIONAL) View the IPv6 prefix list.
<b>ospf</b>	(OPTIONAL) View information for all IPv6 OSPF routes.
<b>rip</b>	(OPTIONAL) View information for all IPv6 RIP routes.
<b>static</b>	(OPTIONAL) View only routes configured by the <code>ipv6 route</code> command.
<b>summary</b>	(OPTIONAL) View a brief list of the configured IPv6 routes.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ipv6 route` command shown in the following examples.

Field	Description
<b>(undefined)</b>	Identifies the type of route: <ul style="list-style-type: none"><li>• L = Local</li><li>• C = connected</li><li>• S = static</li><li>• R = RIP</li><li>• B = BGP</li><li>• IN = internal BGP</li><li>• EX = external BGP</li><li>• LO = Locally Originated</li><li>• O = OSPF</li><li>• IA = OSPF inter-area</li><li>• N1 = OSPF NSSA external type 1</li><li>• N2 = OSPF NSSA external type 2</li><li>• E1 = OSPF external type 1</li><li>• E2 = OSPF external type 2</li><li>• i = IS-IS</li><li>• L1 = IS-IS level-1</li><li>• L2 = IS-IS level-2</li><li>• IA = IS-IS inter-area</li><li>• * = candidate default</li><li>• &gt; = non-active route</li><li>• + = summary routes</li></ul>
<b>Destination</b>	Identifies the route's destination IPv6 address.
<b>Gateway</b>	Identifies whether the route is directly connected and on which interface the route is configured.
<b>Dist/Metric</b>	Identifies if the route has a specified distance or metric.
<b>Last Change</b>	Identifies when the route was last changed or configured.

**Example**

```
Dell#show ipv6 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,
Gateway of last resort is not set
  Destination  Dist/Metric,          Gateway,      Last Change
  -----
C      100::/64 [0/0]
      Direct, Te 0/8, 20:00:18
C      400::/64 [0/0]
      Direct, Tu 1, 00:09:02
```

```

S    800::/64 [1/0]
      via 100::1, Te 0/8, 00:00:50
L    fe80::/10 [0/0]
      Direct, Nu 0, 20:00:18
Dell#

```

**Example  
(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#

```

## trust ipv6-diffserv

Allows the dynamic classification of IPv6 DSCP.

**Syntax** `trust ipv6-diffserv`  
 To remove the definition, use the `no trust ipv6-diffserv` command.

**Defaults** none

**Command Modes** CONFIGURATION-POLICY-MAP-IN

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you configure trust IPv6 diffserv, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Trust diffserv (IPv4) can co-exist with trust ipv6-diffserv in an Input Policy Map. Dynamic classification happens based on the mapping as shown:

IPv6 Service Class Field	Queue ID
<b>111XXXXX</b>	7
<b>110XXXXX</b>	6
<b>101XXXXX</b>	5
<b>100XXXXX</b>	4
<b>011XXXXX</b>	3
<b>010XXXXX</b>	2
<b>001XXXXX</b>	1
<b>000XXXXX</b>	0

# IPv6 Border Gateway Protocol (IPv6 BGP)

IPv6 Border Gateway Protocol (IPv6 BGP) is supported on Dell Networking platforms.

This chapter includes the following sections:

- [IPv6 BGP Commands](#)
- [IPv6 MBGP Commands](#)

## Topics:

- [IPv6 BGP Commands](#)
- [IPv6 MBGP Commands](#)

## IPv6 BGP Commands

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing 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.

The following commands allow you to configure and enable BGP.

### address family

This command changes the context to subsequent address family identifier (SAFI).

**Syntax** `address family ipv6 unicast`  
To remove SAFI context, use the `no address family ipv6 unicast` command.

**Parameters**

<b>ipv6</b>	Enter the keyword <code>ipv6</code> to specify the address family as IPv6.
<b>unicast</b>	Enter the keyword <code>unicast</code> to specify multicast as SAFI.

**Defaults** IPv6 Unicast

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY


**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** After this command is executed, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering the `exit` command and returning to the Router BGP context.

# aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

<b>Syntax</b>	<code>aggregate-address ipv6-address prefix-length [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]</code>	
<b>Parameters</b>	<b>ipv6-address</b> <b>prefix-length</b>	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.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b>advertise-map</b> <b>map-name</b>	(OPTIONAL) Enter the keywords <code>advertise-map</code> then the name of a configured route map to set filters for advertising an aggregate route.
	<b>as-set</b>	(OPTIONAL) Enter the keywords <code>as-set</code> 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.
	<b>attribute-map</b> <b>map-name</b>	(OPTIONAL) Enter the keywords <code>attribute-map</code> then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
	<b>summary-only</b>	(OPTIONAL) Enter the keywords <code>summary-only</code> to advertise only the aggregate address. Specific routes are not advertised.
	<b>suppress-map</b> <b>map-name</b>	(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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS\_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected using the `network` command, that route still appears in the routing table if you configure the `summary-only` parameter 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 ipv6 unicast` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

# bgp always-compare-med

Allows you to enable comparison of the MULTI\_EXIT\_DISC (MED) attributes in the paths from different external ASs.

**Syntax** `bgp always-compare-med`  
To disable comparison of MED, use the `no bgp always-compare-med` command.



**Defaults** Disabled (that is, the software only compares MEDs from neighbors within the same AS).

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Any update without a MED attribute is the least preferred route.  
If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

## 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, use the `no bgp bestpath as-path ignore` command.

**Defaults** Disabled (that is, the software considers the AS\_PATH when choosing a route as best).

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

## bgp bestpath med confed

Enable MULTI\_EXIT\_DISC (MED) attribute comparison on paths learned from BGP confederations.

**Syntax** `bgp bestpath med confed`  
To disable MED comparison on BGP confederation paths, use the `no bgp bestpath med confed` command.

**Defaults** Disabled.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The software compares the MEDs only if the path contains no external autonomous system numbers.  
If you enable this command, use the `capture bgp-pdu max-buffer-size *` command to recompute the best path.

## bgp bestpath med missing-as-best

During path selection, indicate a preference to paths with missing MED (MULTI\_EXIT\_DISC) over those paths with an advertised MED attribute.

<b>Syntax</b>	<code>bgp bestpath med missing-as-best</code> To return to the default selection, use the <code>no bgp bestpath med missing-as-best</code> command.						
<b>Defaults</b>	Disabled.						
<b>Command Modes</b>	ROUTER BGP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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 those with a higher MED.						

## bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

<b>Syntax</b>	<code>bgp client-to-client reflection</code> To disable client-to-client reflection, use the <code>no bgp client-to-client reflection</code> command.						
<b>Defaults</b>	Enabled when a route reflector is configured.						
<b>Command Modes</b>	ROUTER BGP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	Route reflection to clients is not necessary if all client routers are fully meshed.						
<b>Related Commands</b>	<a href="#">bgp cluster-id</a> — assigns an ID to a BGP cluster with two or more route reflectors. <a href="#">neighbor route-reflector-client</a> — configures a route reflector and clients.						

## bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

<b>Syntax</b>	<code>bgp cluster-id {ip-address   number}</code> To delete a cluster ID, use the <code>no bgp cluster-id {ip-address   number}</code> command.				
<b>Parameters</b>	<table><tr><td><b><i>ip-address</i></b></td><td>Enter an IP address as the route reflector cluster ID.</td></tr><tr><td><b><i>number</i></b></td><td>Enter a route reflector cluster ID as a number from 1 to 4294967295.</td></tr></table>	<b><i>ip-address</i></b>	Enter an IP address as the route reflector cluster ID.	<b><i>number</i></b>	Enter a route reflector cluster ID as a number from 1 to 4294967295.
<b><i>ip-address</i></b>	Enter an IP address as the route reflector cluster ID.				
<b><i>number</i></b>	Enter a route reflector cluster ID as a number from 1 to 4294967295.				
<b>Defaults</b>	Not configured.				
<b>Command Modes</b>	ROUTER BGP				

**Supported Modes** Full–Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it displays as an integer.

**Related Commands**

- [bgp client-to-client reflection](#) — enables route reflection between the route reflector and the clients.
- [neighbor route-reflector-client](#) — configures a route reflector and clients.
- [show ip bgp ipv6 unicast 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 1 to 65535.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full–Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGP peers without a LOCAL\_PREF attribute. The software sends AS\_CONFED\_SET and accepts AS\_CONFED\_SET and AS\_CONF\_SEQ.

## bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

**Syntax** `bgp confederation peers as-number [...as-number]`

To remove bgp confederation peers, use the `no bgp confederation peer` command.

**Parameters**

- as-number* Enter the AS number. The range is 1 to 65535.
- ...as-number* (OPTIONAL) Enter up to 16 confederation numbers. The range is from 1 to 65535.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The Autonomous Systems configured in this command are visible to the EBGp neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

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 dampening

Enable BGP route dampening and configure the dampening parameters.

**Syntax**

```
bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]
```

**Parameters**

***half-life***

(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.

***reuse***

(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is **750**.

***suppress***

(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is **2000**.

***max-suppress-time***

(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is **60 minutes**.

***route-map map-name***

(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map. Only match commands in the configured route map are supported.

**Defaults**

Disabled.

**Command Modes**

ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes**

Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you enter `bgp dampening`, the default values for `half-life`, `reuse`, `suppress`, and `max-suppress-time` are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

**Related Commands**

[show ip bgp ipv6 unicast 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

**Syntax** `bgp enforce-first-as`

To turn off the default, use the `no bgp enforce-first-as` command.

**Defaults** Enabled.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the 10/40GbE Switch IO Module.

**Usage Information**

This is enabled by default; that is, for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. To view the failed enforce-first-as check counter, use the `show ip bgp ipv6 unicast neighbors` command.

If you disable `enforce-first-as`, view it using the `show ip protocols` command.

**Related Commands**

[show ip bgp ipv6 unicast neighbors](#) — displays IPv6 routing information exchanged by BGP neighbors.

[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** `bgp fast-external-fallover`

To disable fast external fallover, use the `no bgp fast-external-fallover` command.

<b>Defaults</b>	Enabled.	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	The <code>bgp fast-external-fallover</code> command appears in the <code>show config</code> command output.	

## bgp four-octet-as-support

Enable 4-byte support for the BGP process.

<b>Syntax</b>	<code>bgp four-octet-as-support</code>	
	To disable fast external fallover, use the <code>no bgp four-octet-as-support</code> command.	
<b>Defaults</b>	Disabled (supports 2-Byte format)	
<b>Command Modes</b>	ROUTER BGP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	<p>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.</p> <p>When creating Confederations, all the routers in the Confederation must be 4- or 2-byte identified routers. You cannot mix them.</p> <p>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.</p> <p>For more information about using the 2- or 4-Byte format, refer to the <i>Dell Networking OS Configuration Guide</i>.</p>
--------------------------	--

## bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

<b>Syntax</b>	<code>bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]</code>	
	To return to the default, enter the <code>no bgp graceful-restart</code> command.	
<b>Parameters</b>	<b>neighbor ip-address / peer-group-name</b>	<p>Enter the keyword <code>neighbor</code> then one of the options:</p> <ul style="list-style-type: none"> <li><code>ip-address</code> of the neighbor in IP address format of the neighbor</li> <li><code>peer-group-name</code> of the neighbor peer group</li> </ul>
	<b>restart-time seconds</b>	<p>Enter the keywords <code>restart-time</code> then the maximum number of seconds needed to restart and bring up all peers. The range is from 1 to 3600 seconds. The default is <b>120 seconds</b>.</p>
	<b>stale-path-time seconds</b>	<p>Enter the keywords <code>stale-path-time</code> then the maximum number of seconds to wait before restarting a peer's stale paths. The default is <b>360 seconds</b>.</p>

**role *receiver-only*** Enter the keywords `role receiver-only` to designate the local router to support graceful restart as a receiver only.

**Defaults** As above

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

## bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

**Syntax** `bgp log-neighbor-changes`  
To disable logging, use the `no bgp log-neighbor-changes` command.

**Defaults** Enabled.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The `bgp log-neighbor-changes` command appears in the `show config` command output.

**Related Commands** [show config](#) — views the current configuration.

## bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems (ASs).

**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 does not have their MEDs compared).

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic mode, the path selection for existing paths remains Deterministic until you enter the `capture bgp-pdu max-buffer-size` command to clear existing paths.

## bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

**Syntax** `bgp recursive-bgp-next-hop`  
To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults** Enabled.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

This command is a knob to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

For this command to take effect and to keep the BGP database consistent, you need the `clear ip bgp` command. Execute the `clear ip bgp` command right after executing this command.

**Related Commands** [capture bgp-pdu max-buffer-size](#)

## bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

**Syntax** `bgp regex-eval-optz-disable`  
To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

**Defaults** Enabled.

**Command Modes** ROUTER BGP (conf-router\_bgp)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.



BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expense of RP1 processor memory.

**Related Commands** [show ip protocols](#) — views information on all routing protocols enabled and active.

## bgp router-id

Assign a user-given ID to a BGP router.

**Syntax** `bgp router-id ip-address`  
To delete a user-assigned IP address, use the `no bgp router-id` command.

**Parameters** *ip-address* Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults** The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Peering sessions are reset when you change the router ID of a BGP router.

## bgp soft-reconfig-backup

Use this command *only* when route-refresh is *not* negotiated between peers to avoid having a peer re-send BGP updates.

**Syntax** `bgp soft-reconfig-backup`  
To return to the default setting, use the `no bgp soft-reconfig-backup` command.

**Defaults** **Off**

**Command Modes** ROUTER BGPV6 ADDRESS FAMILY (conf-router\_bgpv6\_af)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router replays and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is *not* negotiated with the peer. If the request is negotiated (after execution of `clear ip bgp soft in`), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

**Related Commands** [clear ip bgp ipv6 unicast soft](#) — activates inbound policies for IPv6 routes without resetting the BGP TCP session.

## capture bgp-pdu neighbor (ipv6)

Enable capture of an IPv6 BGP neighbor packet.

**Syntax** `capture bgp-pdu neighbor ipv6-address direction {both | rx | tx}`  
To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

**Parameters**

<b>ipv6-address</b>	Enter the IPv6 address of the target BGP neighbor.
<b>direction {both   rx   tx}</b>	Enter the keyword <code>direction</code> and a direction — either <code>rx</code> for inbound, <code>tx</code> for outbound, or <code>both</code> .

**Defaults** Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [capture bgp-pdu max-buffer-size](#) — enables route reflection between the route reflector and the clients.
- [show capture bgp-pdu neighbor](#) — configures a route reflector and clients.

## capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

**Syntax** `capture bgp-pdu max-buffer-size 100-102400000`

**Parameters**

<b>100-102400000</b>	Enter a size for the capture buffer.
----------------------	--------------------------------------

**Defaults** **40960000 bytes**

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [capture bgp-pdu neighbor \(ipv6\)](#) — enables route reflection between the route reflector and the clients.
- [show capture bgp-pdu neighbor](#) — configures a route reflector and clients.

## clear ip bgp \* (asterisk)

Reset all BGP sessions in the specified category. The `soft` parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax** `clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast soft [in | out] | soft [in | out]]`

<b>Parameters</b>	<b>*</b>	Enter an asterisk ( * ) to reset all BGP sessions.
	<b>ipv4 multicast soft [in   out]</b>	(OPTIONAL) Enter the keywords <code>ipv4 multicast soft [in   out]</code> to set options within the specified IPv4 address family.
	<b>ipv6 unicast soft [in   out]</b>	(OPTIONAL) Enter the keywords <code>ipv6 multicast soft [in   out]</code> to set options within the specified IPv6 address family.
	<b>soft</b>	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. <b>i</b> <b>NOTE:</b> If you enter <code>clear ip bgp ip6-address soft</code> , both inbound and outbound policies are reset.
	<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
	<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp as-number

Reset BGP sessions. The `soft` parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax**

```
clear ip bgp as-number [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}} | soft [in | out]
```

<b>Parameters</b>	<b>as-number</b>	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is from 1 to 65535.
	<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to clear all flap statistics belonging to that AS or a specified address family within that AS.
	<b>ipv4</b>	(OPTIONAL) Enter the keyword <code>ipv4</code> to select options for that address family.
	<b>ipv6</b>	(OPTIONAL) Enter the keyword <code>ipv6</code> to select options for that address family.
	<b>unicast</b>	(OPTIONAL) Enter the keyword <code>unicast</code> to select the unicast option within the selected address family.
	<b>multicast</b>	(OPTIONAL) Enter the keyword <code>multicast</code> to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
	<b>soft</b>	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration. <b>i</b> <b>NOTE:</b> If you enter <code>clear ip bgp ip6-address soft</code> , both inbound and outbound policies are reset.
	<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
	<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.

**Command Modes** EXEC Privilege


**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax** `clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}}} | ipv6 unicast {flap-statistics | soft {in | out}} | soft [in | out]`

Parameters	Parameter	Description
	<b><i>ipv6-address</i></b>	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword <code>ipv6-address</code> resets all neighbors belonging to that IP.
	<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to clear all flap statistics belonging to that AS or a specified address family within that IP.
	<b>ipv4</b>	(OPTIONAL) Enter the keyword <code>ipv4</code> to select options for that address family.
	<b>ipv6</b>	(OPTIONAL) Enter the keyword <code>ipv6</code> to select options for that address family.
	<b>unicast</b>	(OPTIONAL) Enter the keyword <code>unicast</code> to select the unicast option within the selected address family.
	<b>multicast</b>	(OPTIONAL) Enter the keyword <code>multicast</code> to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
	<b>soft</b>	(OPTIONAL) Enter the keyword <code>soft</code> to configure and activate policies without resetting the BGP TCP session; that is, BGP Soft Reconfiguration.  <b>NOTE:</b> If you enter <code>clear ip bgp ip6-address soft</code> , both inbound and outbound policies are reset.
	<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to activate only inbound policies.
	<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to activate only outbound policies.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp peer-group

Reset a peer-group's BGP sessions.

**Syntax** `clear ip bgp peer-group peer-group-name`

**Parameters** ***peer-group-name*** Enter the peer group name to reset the BGP sessions within that peer group.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch


Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

**Syntax** `clear ip bgp ipv6 unicast dampening [ipv6-address]`

**Parameters** *ipv6-address* 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.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** After you enter this command, the software deletes the history routes and returns the suppressed routes to the active state.

## clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

**Syntax** `clear ip bgp ipv6 unicast flap-statistics [ipv6-address | filter-list as-path-name | regexp regular-expression]`

**Parameters** *ipv6-address* (OPTIONAL) Enter the IPv6 address in the x:x:x::x 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.

*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 the regular expressions. Use one or a combination of the following:

- . (period) matches on any single character, including white space
- \* (asterisk) matches on sequences in a pattern (zero or more sequences)
- + (plus sign) matches on sequences in a pattern (one or more sequences)
- ? (question mark) matches sequences in a pattern (0 or 1 sequences)
- [ ] (brackets) matches a range of single-character patterns.
- ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- \$ (dollar sign) matches the end of the output string.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you enter the `clear ip bgp ipv6 flap-statistics` command without parameters, all the statistics clear.

**Related Commands** [show ip bgp ipv6 unicast flap-statistics](#) — views BGP flap statistics.

## clear ip bgp ipv6 unicast soft

Clear and reapply policies for IPv6 unicast routes without resetting the TCP connection; that is, perform BGP soft reconfiguration.


<b>Syntax</b>	<code>clear ip bgp {*   as-number   ipv4-neighbor-addr   ipv6-neighbor-addr   peer-group name} ipv6 unicast soft [in   out]</code>	
<b>Parameters</b>	<b>*</b>	Clear and reapply policies for all BGP sessions.
	<b>as-number</b>	Clear and reapply policies for all neighbors belonging to the AS. The range is from 0 to 65535 (2 Byte), from 1 to 4294967295 (4 Byte), or from 0.1 to 0.65535.65535 (Dotted format).
	<b>ipv4-neighbor-addr   ipv6-neighbor-addr</b>	Clear and reapply policies for a neighbor.
	<b>peer-group name</b>	Clear and reapply policies for all BGP routers in the specified peer group.
	<b>ipv6 unicast</b>	Clear and reapply policies for all IPv6 unicast routes.
	<b>in</b>	Reapply only inbound policies.  <b>NOTE:</b> If you enter <code>soft</code> , without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.
	<b>out</b>	Reapply only outbound policies.  <b>NOTE:</b> If you enter <code>soft</code> , without an <code>in</code> or <code>out</code> option, both inbound and outbound policies are reset.
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ip bgp

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

<b>Syntax</b>	<code>debug ip bgp [ipv6-address   peer-group peer-group-name] [in   out]</code>	
	To disable all BGP debugging, use the <code>no debug ip bgp</code> command.	
<b>Parameters</b>	<b>ipv6-address</b>	(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.

**peer-group *peer-group-name*** Enter the keywords `peer-group` then the name of the peer group.

**in** (OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.

**out** (OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 `debug ip bgp in` and then enter `debug ip bgp out`, 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.

## debug ip bgp events


Allows you to view information on local BGP state changes and other BGP events.

**Syntax** `debug ip bgp [ipv6-address | peer-group peer-group-name] events [in | out]`

To disable debugging, use the `no debug ip bgp ipv6-address | peer-group peer-group-name] events` command.

**Parameters**

***ipv6-address*** (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.

**peer-group *peer-group-name*** Enter the keywords `peer-group` then the name of the peer group.

**in** (OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.

**out** (OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

## debug ip bgp ipv6 dampening

View information on dampened (non-active) IPv6 routes.

**Syntax** `debug ip bgp ipv6 unicast dampening [in | out]`  
 To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

**Parameters**

- in** (OPTIONAL) Enter the keyword `in` to view only inbound dampened routes.
- out** (OPTIONAL) Enter the keyword `out` to view only outbound dampened routes.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

**Related Commands** [show ip bgp ipv6 unicast dampened-paths](#) — views BGP dampened routes.

## debug ip bgp ipv6 unicast soft-reconfiguration

Enable soft-reconfiguration debugging for IPv6 unicast routes.

**Syntax** `debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration`  
 To disable debugging, use the `no debug ip bgp [ipv4-address | ipv6-address | peer-group-name] ipv6 unicast soft-reconfiguration` command.

**Parameters**

- ipv4-address | ipv6-address** Enter the IP address of the neighbor on which you want to enable soft-reconfiguration debugging.
- peer-group-name** Enter the name of the peer group on which you want to enable soft-reconfiguration debugging.
- ipv6 unicast** Debug soft reconfiguration for IPv6 unicast routes.

**Defaults** Disabled.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.



**Usage Information** This command turns on BGP soft-reconfiguration inbound debugging for IPv6 unicast routes. If no neighbor is specified, debug is turned on for all neighbors.

**Related Commands** [show ip bgp ipv6 unicast dampened-paths](#) — views BGP dampened routes.


## debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

**Syntax** `debug ip bgp [ipv6-address | peer-group peer-group-name] keepalives [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

**Parameters**

**ipv6-address** (OPTIONAL) Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is /0 to /128.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**peer-group peer-group-name** (OPTIONAL) Enter the keywords `peer-group` then the name of the peer group.

**in** (OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.

**out** (OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Entering a `no debug ip bgp` command removes all configured debug commands for BGP.


## debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

**Syntax** `debug ip bgp [ipv6-address | peer-group peer-group-name] notifications [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

**Parameters**

**ipv6-address** (OPTIONAL) Enter the IPv6 address in the x:x:x:x 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.

**peer-group peer-group-name** (OPTIONAL) Enter the keywords `peer-group` then the name of the peer group.

**in** (OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.

**out** (OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

## debug ip bgp updates

Allows you to view information about BGP updates.

**Syntax** `debug ip bgp [ipv6-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out]` command.

Parameters		
<b>ipv6-address</b>	(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.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group peer-group-name</b>	(OPTIONAL) Enter the keywords <code>peer-group</code> then the name of the peer group.	
<b>ipv6 unicast [ipv6-address]</b>	(OPTIONAL) Enter the keywords <code>ipv6 unicast</code> , and, optionally, an ipv6 address.	
<b>in</b>	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.	
<b>out</b>	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.	

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

## default-metric

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The `default-metric` command in BGP sets the value of the BGP MULTI\_EXIT\_DISC (MED) attribute for redistributed routes only.

**Related Commands** [bgp always-compare-med](#) — enables comparison of all BGP MED attributes.  
[redistribute](#) — redistributes routes from other routing protocols into BGP.

## description

Enter a description of the BGP routing protocol.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [router bgp](#) — enters ROUTER mode on the switch.

## distance bgp

Configure three administrative distances for routes.

**Syntax** `distance bgp external-distance internal-distance local-distance`  
To return to default values, use the `no distance bgp` command.

**Parameters** **external-distance** Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.

**internal-distance** Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.


**local-distance** Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

**Defaults**

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	 <b>CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.</b>	
	<p>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.</p> <p>Routes from confederations are treated as internal BGP routes.</p>	


## maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

<b>Syntax</b>	<code>maximum-paths {ebgp   ibgp} number</code>	
	To return to the default values, use the <code>no maximum-paths</code> command.	
<b>Parameters</b>	<b>ebgp</b>	Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.
	<b>ibgp</b>	Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes.
	<b>number</b>	Enter a number as the maximum number of parallel paths. The range is from 1 to 16. The default is <b>1</b> .
<b>Defaults</b>	<b>1</b>	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	If you enable this command, use the <code>capture bgp-pdu max-buffer-size</code> command to recompute the best path.	

## neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

<b>Syntax</b>	<code>neighbor {ipv6-address   peer-group-name} activate</code>	
	To disable, use the <code>no neighbor {ipv6-address   peer-group-name} activate</code> command.	
<b>Parameters</b>	<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x::x format.  <b>NOTE:</b> The <code>::</code> notation specifies successive hexadecimal fields of zeros.
	<b>peer-group-name</b>	Identify a peer group by name.
	<b>activate</b>	Enter the keyword <code>activate</code> to enable the identified neighbor or peer group in the new AFI/SAFI.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** By default, when you create a neighbor/peer group configuration in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.

## neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

**Syntax** `neighbor {ipv6-address | peer-group-name} advertisement-interval seconds`  
To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

**Parameters**

- ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name** Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- seconds** Enter a number as the time interval, in seconds, between BGP advertisements. The range is 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 BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch


<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

**Syntax** `neighbor {ip-address | peer-group-name} allowas-in number`  
To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

**Parameters**

- ip-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name** Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- number** Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**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** `neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]` command.

Parameters		
<b><i>ipv6-address</i></b>	Enter the IPv6 address in the x:x:x::x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b><i>peer-group-name</i></b>	Enter the name of the peer group to set the default route of all routers in that peer group.	
<b><i>route-map map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.	

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

## neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

**Syntax** `neighbor {ipv6-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ipv6-address | peer-group-name} description text` command.

Parameters		
<b><i>ipv6-address</i></b>	Enter the IPv6 address in the x:x:x::x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b><i>peer-group-name</i></b>	Enter the name of the peer group.	
<b><i>text</i></b>	Enter a continuous text string up to 80 characters.	

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor distribute-list

Distribute BGP information using an established prefix list.

**Syntax** `neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group.	
<b>prefix-list-name</b>	Enter the name of an established prefix list. If the prefix list is not configured, the default is <b>permit</b> (to allow all routes).	
<b>in</b>	Enter the keyword in to distribute only inbound traffic.	
<b>out</b>	Enter the keyword out to distribute only outbound traffic.	

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [neighbor filter-list](#) — assigns a AS-PATH list to a neighbor or peer group.  
[neighbor route-map](#) — assigns a route map to a neighbor or peer group.

## neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

**Syntax** `neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]`  
To disallow and disconnect connections, use the `no neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** To prevent loops, the `neighbor ebgp-multihop` command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

## neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

**Syntax** `neighbor {ipv6-address | peer-group-name} fall-over`  
To disable, use the `no neighbor {ipv6-address | peer-group-name} fall-over` command.

**Parameters**

- ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name** Enter the name of the peer group.

**Defaults** Disabled.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable fall-over, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.


**Related Commands** [show ip bgp ipv6 unicast neighbors](#) — displays IPv6 routing information exchanged by BGP neighbors.

## neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

**Syntax** `neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}`  
To delete a BGP filter, use the `no neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}` command.

**Parameters**

- ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.



**peer-group-name** Enter the name of the peer group to apply the filter to all routers in the peer group.

**in** Enter the keyword `in` to filter inbound BGP routes.

**out** Enter the keyword `out` to filter outbound BGP routes.

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


## neighbor maximum-prefix

Control the number of network prefixes received.

**Syntax** `neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**peer-group-name** Enter the name of the peer group.

**maximum** Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.

**threshold** (OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is **75**.

**warning-only** (OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

**Defaults** threshold = **75**

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp ipv6 unicast summary` command displays (prfxcd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `capture bgp-pdu max-buffer-size` command for the neighbor or the peer group to which the neighbor belongs or you enter `neighbor shutdown` and `neighbor no shutdown` commands.

**Related Commands** [show ip bgp ipv6 unicast summary](#) — displays the current BGP configuration.

## neighbor X:X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

**Syntax** `neighbor x:x:x::x password {7 <encrypt-pass> | <clear-pass>}`  
To return to the default setting, use the `no neighbor x:x:x::x password` command.

**Parameters**

<b><i>encrypt-pass</i></b>	Enter the encrypted password.
<b><i>clear-pass</i></b>	Enter the clear text password.

**Defaults** Disabled.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** The TCP session is authentication and prevents the data from being compromised.

## neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

**Syntax** `neighbor {ipv6-address | peer-group-name} next-hop-self`  
To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self` command.

**Parameters**

<b><i>ipv6-address</i></b>	Enter the IPv6 address in the x:x:x::x format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b><i>peer-group-name</i></b>	(OPTIONAL) Enter the name of the peer group.

**Defaults** Disabled.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

## neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

**Syntax** `neighbor ipv6-address peer-group peer-group-name`  
To delete a peer from a peer group, use the `no neighbor ipv6-address peer-group peer-group-name` command.

<b>Parameters</b>	<b><i>ipv6-address</i></b>	Enter the IPv6 address in the x:x:x:x format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b><i>peer-group peer-group-name</i></b>	Enter the keywords <code>peer-group</code> then the name of a configured peer group (maximum 16 characters).

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- [neighbor advertisement-interval](#)
- [neighbor distribute-list](#)
- [neighbor filter-list](#)
- [neighbor next-hop-self](#)
- [neighbor route-map](#)
- [neighbor route-reflector-client](#)
- [neighbor send-community](#)

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (`shutdown`) the peers within the group are also disabled (`shutdown`).

**Related Commands**

- [capture bgp-pdu max-buffer-size](#) — resets BGP sessions.
- [neighbor peer-group \(creating group\)](#) — creates a peer group.
- [show ip bgp ipv6 unicast peer-group](#) — views BGP peers.
- [show ip bgp ipv6 unicast 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** ***peer-group-name*** Enter a text string up to 16 characters long as the name of the peer group.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When a peer group is created, it is disabled (`shut mode`).

**Related Commands** [neighbor peer-group \(assigning peers\)](#) — assigns routers to a peer group.  
[neighbor remote-as](#) — assigns an indirectly connected AS to a neighbor or peer group.  
[neighbor shutdown](#) — disables a peer or peer group.

## neighbor peer-group passive

Enable passive peering on a BGP peer group; that is, the peer group does not send an OPEN message, but does respond to one.

**Syntax** `neighbor peer-group-name peer-group passive`  
To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

**Parameters** **peer-group-name** Enter a text string up to 16 characters long as the name of the peer group.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** After you configure a peer group as passive, you must assign it a subnet using the `neighbor subnet` command.

**Related Commands** [neighbor subnet](#) — assigns a subnet to a dynamically configured BGP neighbor.

## neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

**Syntax** `neighbor {ipv6-address | peer-group-name} remote-as number`  
To delete a remote AS entry, use the `no neighbor {ipv6-address | peer-group-name} remote-as number` command.

**Parameters** **ipv6-address** Enter the IPv6 address in the x:x:x::x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.  
**peer-group-name** Enter a text string up to 16 characters long as the name of the peer group.  
**number** Enter a number of the AS. The range is from 1 to 65535.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (`shutdown`).


**Related Commands** `router bgp` — enters the ROUTER BGP mode and configure routes in an AS.

## neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

**Syntax** `neighbor {ipv6-address | peer-group-name} remove-private-as`  
To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

**Parameters**

***ipv6-address*** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

***peer-group-name*** Enter the name of the peer group to remove the private AS numbers.

**Defaults** Disabled (that is, the private AS number are not removed).

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Applies to external border gateway protocol (EBGP) neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.


Private AS numbers are from 64512 to 65535.

## neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

**Syntax** `neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}`  
To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

**Parameters**

***ipv6-address*** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

***peer-group-name*** Enter the name of the peer group.

***map-name*** Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).


***in*** Enter the keyword `in` to filter inbound routes.

***out*** Enter the keyword `out` to filter outbound routes.

<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.</p> <p>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.</p>	

## neighbor route-reflector-client


Configure a neighbor as a member of a route reflector cluster.

<b>Syntax</b>	<code>neighbor {ipv6-address   peer-group-name} route-reflector-client</code>	
	To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the <code>no neighbor {ipv6-address   peer-group-name} route-reflector-client</code> command.	
<b>Parameters</b>	<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x:x format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b>peer-group-name</b>	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.</p> <p>When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.</p>	

## 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.

<b>Syntax</b>	<code>neighbor {ipv6-address   peer-group-name} send-community</code>	
	To disable sending a COMMUNITY attribute, use the <code>no neighbor {ipv6-address   peer-group-name} send-community</code> command.	
<b>Parameters</b>	<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x:x format.

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

**peer-group-name** Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

**Defaults** Not configured and COMMUNITY attributes are not sent to neighbors.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor shutdown

Disable a BGP neighbor or peer group.

**Syntax** `neighbor {ipv6-address | peer-group-name} shutdown`  
To enable a disabled neighbor or peer group, use the `no neighbor {ipv6-address | peer-group-name} shutdown` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**peer-group-name** Enter the name of the peer group to disable or enable all routers within the peer group.

**Defaults** Enabled (that is, BGP neighbors and peer groups are disabled.)

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Peers that are enabled within a peer group are disabled when their peer group is disabled.  
The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp ipv6 unicast summary` command to confirm its status.

**Related Commands** [show ip bgp ipv6 unicast summary](#) — displays the current BGP configuration.  
[show ip bgp ipv6 unicast neighbors](#) — displays IPv6 routing information exchanged by BGP neighbors.

## neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

**Syntax** `neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound`

**Parameters**

***ipv4-address* | *ipv6-address*** Enter the IP address of the neighbor for which you want to start storing inbound routing updates.

***peer-group-name*** Enter the name of the peer group for which you want to start storing inbound routing updates.


**Defaults** Disabled.

**Command Modes** ROUTER BGPv6 ADDRESS FAMILY (conf-router\_bgpv6\_af)

**Supported Modes** Full–Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command enables soft-reconfiguration for the specified BGP neighbor. BGP stores all updates for inbound IPv6 unicast routes the neighbor receives but does not reset the peer-session.

 **CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.**

**Related Commands** [show ip bgp ipv6 unicast neighbors](#) — displays IPv6 routing information BGP neighbors exchange.

## neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

**Syntax** `neighbor peer-group-name subnet subnet-number mask`

To remove passive peering, use the `no neighbor peer-group-name subnet subnet-number mask` command.

**Parameters**

***subnet-number*** Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0 : : 0 / 0.

***mask*** Enter a prefix mask in / prefix-length format (/x).

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full–Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.


**Syntax** `neighbor {ipv6-address | peer-group-name} timers keepalive holdtime`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} timers` command.

**Parameters**

***ipv6-address*** Enter the IPv6 address in the x:x:x:x::x format.



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

- peer-group-name*** Enter the name of the peer group to set the timers for all routers within the peer group.
- keepalive*** Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. the range is from 1 to 65535. the default is **60 seconds**.
- holdtime*** Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

- Defaults**
- keepalive = **60 seconds**
  - holdtime = **180 seconds**

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different keepalive and holdtime values, negotiate for new values, the resulting values are as follows:


- the lower of the holdtime values is the new holdtime value
- whichever is the lower value; one-third of the new holdtime value, or the configured keepalive value is the new keepalive value

## neighbor update-source

Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

**Syntax** `neighbor {ipv6-address | peer-group-name} update-source loopback interface`

To use the closest interface, use the `no neighbor {ipv6-address | peer-group-name} update-source loopback interface` command.

- Parameters**
- ipv6-address*** Enter the IPv6 address in the x:x:x::x format.
-  **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.
- peer-group-name*** Enter the name of the peer group to set the timers for all routers within the peer group.
- loopback interface*** Enter the keyword `loopback` then a number of the loopback interface. The range is from 0 to 16383.

**Defaults** Not configured.

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

## neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

**Syntax** `neighbor {ipv6-address | peer-group-name} weight weight`  
To remove a weight value, use the `no neighbor {ipv6-address | peer-group-name} weight weight` command.

**Parameters**

<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format. <b>i</b> <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group to set the timers for all routers within the peer group.
<b>weight</b>	Enter a number as the weight. The range is from 0 to 65535. The default is <b>0</b> .

**Defaults** 0

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** In the system best path selection process, the path with the highest weight value is preferred.  
**i** **NOTE:** To apply the weight to the connection and recompute the best path, reset the neighbor connection (the `capture bgp-pdu max-buffer-size * command`).

## network

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax** `network ipv6-address prefix-length [route-map map-name]`  
To remove a network, use the `no network ip-address mask [route-map map-name]` command.

**Parameters**

<b>ipv6-address</b> <b>prefix-length</b>	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. <b>i</b> <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>mask</b>	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).
<b>route-map map-name</b>	(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 <b>deny</b> (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

<b>Command History</b>	<p><b>Version</b></p> <p><b>9.9(0.0)</b> Introduced on the FN IOM.</p> <p><b>9.2(0.0)</b> Introduced on the MXL 10/40GbE Switch IO Module.</p>	<b>Description</b>
<b>Usage Information</b>	The software resolves the network address configured by the <code>network</code> command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.	
<b>Related Commands</b>	<code>redistribute</code> — redistributes routes into BGP.	

## network backdoor

Specify this IGP route as the preferred route.


**Syntax** `network ipv6-address prefix-length backdoor`

To remove a network, use the `no network ipv6-address prefix-length backdoor` command.

**Parameters**

**ipv6-address** 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.

**prefix-length**

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

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

<b>Command History</b>	<p><b>Version</b></p> <p><b>9.9(0.0)</b> Introduced on the FN IOM.</p> <p><b>9.2(0.0)</b> Introduced on the MXL 10/40GbE Switch IO Module.</p>	<b>Description</b>
------------------------	--	--------------------

**Usage Information** Though the system does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

## redistribute

Redistribute routes into BGP.

**Syntax** `redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

**Parameters**

**connected** Enter the keyword `connected` to redistribute routes from physically connected interfaces.

**static** Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.

**route-map map-name** (OPTIONAL) Enter the keywords `route-map` then the name of an established route map.

If the route map is not configured, the default is **deny** (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0::0/0), configure the `neighbor default-originate` command.

**Related Commands**

[neighbor default-originate](#) — injects the default route.

## redistribute isis

Redistribute IS-IS routes into BGP.

**Syntax**

```
redistribute isis [level-1 | level-1-2 | level-2] [metric metric-value | metric-type {external | internal}] [route-map map-name]
```

To stop redistribution of IS-IS routes, use the `no redistribute isis` command.

**Parameters**

<b>level-1   level-1-2   level-2</b>	(OPTIONAL) Enter the type (level) of routes to redistribute.
<b>metric</b>	(OPTIONAL) Assign metric to an interface for use with IPv6 information.
<b>metric-type</b>	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following: <ul style="list-style-type: none"> <li>• external</li> <li>• <b>internal</b> (default)</li> </ul>
<b>route-map map-name</b>	(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 <b>deny</b> (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## redistribute ospf

Redistribute OSPFv3 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**

<b>process-id</b>	Enter the number of the OSPFv3 process. The range is from 1 to 65535.
<b>match external {1   2}</b>	(OPTIONAL) Enter the keywords <code>match external</code> to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.

<b>match internal</b>	(OPTIONAL) Enter the keywords <code>match internal</code> to redistribute OSPFv3 internal routes only.
<b>route-map <i>map-name</i></b>	(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 <b>deny</b> (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enter the `redistribute ospf process-id` command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

## router bgp

Enter ROUTER BGP mode to configure and enable BGP.

**Syntax** `router bgp as-number`  
To disable BGP, use the `no router bgp as-number` command.

**Parameters** ***as-number*** Enter the AS number. The range is from 1 to 65535.

**Defaults** Not enabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv6 address.

**Syntax** `show capture bgp-pdu neighbor ipv6-address`

**Parameters** ***ipv6-address*** Enter the IPv6 address (X:X:X::X) of a BGP neighbor.

**Defaults**

- EXEC
- EXEC Privilege

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Command** [capture bgp-pdu neighbor \(ipv6\)](#) — enables capture of an IPv6 BGP neighbor packet.  
[capture bgp-pdu max-buffer-size](#) — specifies a size for the capture buffer.

## show config

View the current ROUTER BGP configuration.

**Syntax** `show config`

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown

!
Dell#
```

## show ip bgp ipv6 unicast

View the current BGP information.

**Syntax** `show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]`

Parameters		
<b>network</b>	(OPTIONAL)	Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
<b>network-mask</b>	(OPTIONAL)	Enter the keywords <code>network mask</code> (in slash prefix format) of the BGP network address.
<b>longer-prefixes</b>	(OPTIONAL)	Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

## show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast cluster-list [cluster-id]</code>	
<b>Parameters</b>	<b>cluster-id</b>	(OPTIONAL) Enter the cluster id in dotted decimal format.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]</code>	
<b>Parameters</b>	<b>community-number</b>	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.
	<b>local-AS</b>	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 (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
	<b>no-advertise</b>	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 (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
	<b>no-export</b>	Enter the keywords <code>no-export</code> to view 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.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

## show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

**Syntax** `show ip bgp ipv6 unicast community-list community-list-name [exact-match]`

**Parameters**

<b><i>community-list-name</i></b>	Enter the name of a configured IP community list.
<b>exact-match</b>	(OPTIONAL) Enter the keywords <code>exact-match</code> to display only for an exact match of the communities.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

**Syntax** `show ip bgp ipv6 unicast dampened-paths`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast detail

Display BGP internal information for IPv6 Unicast address family.

**Syntax** `show ip bgp ipv6 unicast detail`

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.



## show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

**Syntax** `show ip bgp ipv6 unicast extcommunity-list [list name]`

**Parameters** **list name** Enter the extended community list name you wish to view.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp ipv6 unicast 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 ipv6 unicast` command output.

## show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

**Syntax** `show ip bgp ipv6 unicast filter-list as-path-name`

**Parameters** **as-path-name** Enter the name of an AS-PATH.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

**Syntax** `show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list as-path-name] [regexp regular-expression]`


**Parameters** **ipv6-address prefix-length** Enter the IPv6 address in the x:x:x:x 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.

**filter-list as-path-name** (OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH ACL.

### **regexp *regular-expression***

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
  - `*` = (asterisk) the sequences in a pattern (0 or more sequences).
  - `+` = (plus) the sequences in a pattern (1 or more sequences).
  - `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).
-  **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
  - `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - `$` = (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

**Syntax** `show ip bgp ipv6 unicast inconsistent-as`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast neighbors

Displays information on IPv6 unicast routes exchanged by BGP neighbors.

**Syntax** `show ip bgp ipv6 unicast neighbors [ipv4-neighbor-addr | ipv6-neighbor-addr] [advertised-routes | dampened-routes | detail | flap-statistics | routes | received-routes [network [network-mask]] | denied-routes [network [network-mask]]]`

**Parameters**

- ipv6 unicast** Enter the keywords `ipv6 unicast` to view information only related to IPv6 unicast routes.
- ipv4-neighbor-addr | ipv6-neighbor-addr** (OPTIONAL) Enter the IP address of the neighbor to view only BGP route information exchanged with that neighbor.
- advertised-routes** (OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.

<b>dampened-routes</b>	(OPTIONAL) Enter the keywords <code>dampened-routes</code> to view information on dampened routes from the BGP neighbor.
<b>detail</b>	(OPTIONAL) Enter the keyword <code>detail</code> to view neighbor-specific internal information for the IPv4 Unicast address family.
<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to view flap statistics on the neighbor's routes.
<b>routes</b>	(OPTIONAL) Enter the keyword <code>routes</code> to view only the neighbor's feasible routes.
<b>received-routes</b> <b>[<i>network</i>]</b> <b>[<i>network-mask</i>]</b>	(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.  <b>i</b> <b>NOTE:</b> You must configure the <code>neighbor soft-reconfiguration inbound</code> command prior to viewing all the information received from the neighbors.
<b>denied-routes</b> <b>[<i>network</i>]</b> <b>[<i>network-mask</i>]</b>	(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 using neighbor inbound filters.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning With	Description
<b>BGP neighbor</b>	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, then the link is internal; otherwise, the link is external.
<b>BGP version</b>	Displays the BGP version (always version 4) and the remote router ID.
<b>BGP state</b>	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
<b>Last read</b>	This line displays the following information: <ul style="list-style-type: none"> <li>• last read is the time (hours:minutes:seconds) the router reads a message from its neighbor</li> <li>• hold time is the number of seconds configured between messages from its neighbor</li> <li>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive</li> </ul>
<b>Received messages</b>	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.
<b>Sent messages</b>	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.
<b>Received updates</b>	This line displays the number of BGP updates received and sent.

Lines Beginning With	Description
<b>Soft reconfiguration</b>	This line indicates that soft reconfiguration inbound is configured.
<b>Minimum time</b>	Displays the minimum time, in seconds, between advertisements.
<b>(List of inbound and outbound policies)</b>	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
<b>For address family:</b>	Displays IPv6 Unicast as the address family.
<b>BGP table version</b>	Displays which version of the primary BGP routing table the router and the neighbor are using.
<b>Prefixes accepted</b>	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
<b>Prefixes advertised</b>	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
<b>Connections established</b>	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
<b>Last reset</b>	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.
<b>Local host:</b>	Displays the peering address of the local router and the TCP port number.
<b>Foreign host:</b>	Displays the peering address of the neighbor and the TCP port number.

### Example

```
Dell#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 3; dropped 2
Last reset 00:00:39, due to Closed by neighbor
```

```

Notification History
  'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:10::4, Local port: 179
Foreign host: 5ffe:10::3, Foreign port: 35470

Notification History
  'Connection Reset' Sent : 1 Recv: 0

BGP neighbor is 5ffe:11::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:28
  Last read 00:00:28, last write 00:00:28
  Hold time is 180, keepalive interval is 60 seconds
  Received 27 messages, 3 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Received 8 updates, Sent 0 updates
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)
Capabilities advertised to neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
BGP table version 12, neighbor version 12
2 accepted prefixes consume 32 bytes

Prefix advertised 0, rejected 0, withdrawn 0
Connections established 3; dropped 2
Last reset 00:00:41, due to Closed by neighbor

Notification History
  'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:11::4, Local port: 179

```

## show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]</code>				
<b>Parameters</b>	<p><b>peer-group-name</b> (OPTIONAL) Enter the name of a peer group to view information about that peer group only.</p> <p><b>detail</b> (OPTIONAL) Enter the keyword <code>detail</code> to view peer-group-specific information for the IPv6 address family.</p> <p><b>summary</b> (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 ipv6 unicast summary</code> command.</p>				
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	<table border="0" style="width: 100%;"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.
Version	Description				
<b>9.9(0.0)</b>	Introduced on the FN IOM.				

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
Dell#
```

## show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

**Syntax** show ip bgp ipv6 unicast summary

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor AS      MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/Pfx
1109::33  18508  0        0        0      0      0      never  Active
2222::220 18508  0        0        0      0      0      never  Active
4000::33  18508  0        0        0      0      0      never  Active
4000::60  18508  0        0        0      0      0      never  Active
9000::4:2 18508  0        0        0      0      0      never  Active
9000::5:2 1      35       32       0      0      0      00:16:42  0
9000::6:2 2      35       32       0      0      0      00:16:39  0
9000::7:2 3      35       32       0      0      0      00:16:41  0
9000::8:2 18508  35       32       0      0      0      00:16:42  0
9000::9:2 18508  44       19       0      0      0      00:16:41  0
9000::a:2 18508  35       32       0      0      0      00:16:43  0
9000::b:14 18508  29       29       0      0      0      00:13:01  0
Dell#
```

## 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.


<b>Syntax</b>	show ip bgp next-hop [local-routes]	
<b>Parameters</b>	<b>local-routes</b>	(OPTIONAL) Show next-hop information for local routes.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ip bgp next-hop
Next-hop      Via                RefCount  Cost  Flaps  Time Elapsed
9000::5:2     9000::5:2, Gi 8/38  2          0    0    00:23:22
9000::6:2     9000::6:2, Gi 8/38  2          0    0    00:23:22
9000::7:2     9000::7:2, Gi 8/38  2          0    0    00:23:22
9000::8:2     9000::8:2, Gi 8/38  2          0    0    00:23:22
9000::9:2     9000::9:2, Gi 8/38 6000       0    0    00:23:16
9000::a:2     9000::a:2, Gi 8/38  2          0    0    00:23:22
Dell#
```

## show ip bgp paths

View all the BGP path attributes in the BGP database.

<b>Syntax</b>	show ip bgp paths [regexp regular-expression]	
<b>Parameters</b>	<b>regexp regular-expression</b>	Enter a regular expression then use one or a combination of the following characters to match: <ul style="list-style-type: none"><li>. = (period) any single character (including a white space).</li><li>* = (asterisk) the sequences in a pattern (0 or more sequences).</li><li>+ = (plus) the sequences in a pattern (1 or more sequences).</li><li>? = (question mark) sequences in a pattern (either 0 or 1 sequences).</li><li> <b>NOTE:</b> You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.</li><li>[ ] = (brackets) a range of single-character patterns.</li><li>^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.</li><li>\$ = (dollar sign) the end of the output string.</li></ul>
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

**Syntax** `show ip bgp paths as-path`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

**Syntax** `show ip bgp paths community`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp paths extcommunity

View all unique extended community information in the BGP database.

**Syntax** `show ip bgp paths extcommunity`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp regexp


Allows you to view the subset of BGP routing table matching the regular expressions specified.

**Syntax** `show ip bgp regexp regular-expression [character]`

**Parameters**

<b><i>regular-expression</i></b> <b>[<i>character</i>]</b>	Enter a regular expression then use one or a combination of the following characters to match: <ul style="list-style-type: none"><li>• . = (period) any single character (including a white space).</li><li>• * = (asterisk) the sequences in a pattern (0 or more sequences).</li></ul>
---	--



- + = (plus) the sequences in a pattern (1 or more sequences).
- ? = (question mark) sequences in a pattern (either 0 or 1 sequences).
-  **NOTE:** You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.
- [ ] = (brackets) a range of single-character patterns.
- ^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- \$ = (dollar sign) the end of the output string.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## timers bgp

Allows you to adjust the BGP network timers for all neighbors.

**Syntax** `timers bgp keepalive holdtimer`  
 To return to the default values, use the `no timers bgp` command.

**Parameters**

<b><i>keepalive</i></b>	Enter the time interval (in seconds) between which the system sends keepalive messages. The range is from 1 to 65535. The default is <b>60 seconds</b> .
<b><i>holdtimer</i></b>	Enter the time interval (in seconds) that the the system waits since the last keepalive message before declaring a BGP peer dead. The range is from 3 to 65535. The default is <b>180 seconds</b> .

**Defaults**

- keepalive = **60 seconds**
- holdtimer = **180 seconds**

**Command Modes** ROUTER BGP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [neighbor timers](#) — adjusts BGP timers for a specific peer or peer group.

# IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). The Dell Networking MBGP is implemented as per IETF RFC 1858.


## address family

This command changes the context to subsequent address family identifier (SAFI).

<b>Syntax</b>	<code>address family ipv6 unicast</code> To remove SAFI context, use the <code>no address family ipv6 unicast</code> command.						
<b>Parameters</b>	<b>ipv6</b> Enter the keyword <code>ipv6</code> to specify the address family as IPv6. <b>unicast</b> Enter the keyword <code>unicast</code> to specify multicast as SAFI.						
<b>Defaults</b>	IPv6 Unicast						
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	After this command is executed, all subsequent commands apply to this address family. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering the <code>exit</code> command and returning to the Router BGP context.						

## aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

<b>Syntax</b>	<code>aggregate-address ipv6-address prefix-length [advertise-map map-name] [as-set] [attribute-map map-name] [summary-only] [suppress-map map-name]</code>
<b>Parameters</b>	<b>ipv6-address</b> <b>prefix-length</b> 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.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b>advertise-map</b> <b>map-name</b> (OPTIONAL) Enter the keywords <code>advertise-map</code> then the name of a configured route map to set filters for advertising an aggregate route.
	<b>as-set</b> (OPTIONAL) Enter the keywords <code>as-set</code> 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.
	<b>attribute-map</b> <b>map-name</b> (OPTIONAL) Enter the keywords <code>attribute-map</code> then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
	<b>summary-only</b> (OPTIONAL) Enter the keywords <code>summary-only</code> to advertise only the aggregate address. Specific routes are not advertised.
	<b>suppress-map</b> <b>map-name</b> (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.
<b>Defaults</b>	Not configured.

**Command Modes** ROUTER-BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate. If routes within the aggregate are constantly changing, 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 true: routes meeting the `permit` clause are suppressed.

If the route is injected using the `network` command, that route stills appear 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.

## bgp dampening

Enable MBGP route dampening.

**Syntax**

```
bgp dampening [half-life time] [route-map map-name]
```

To disable route dampening, use the `no bgp dampening [half-life time] [route-map map-name]` command.

**Parameters**

<b><i>half-life time</i></b>	(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 <b>15 minutes</b> .
<b><i>route-map map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map. Only match commands in the configured route map are supported.

**Defaults**

Disabled.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp ipv6 unicast


Reset MBGP sessions.

**Syntax**

```
clear ip bgp ipv6 unicast * ipv6-address prefix-length [dampening | flap-statistics] peer-group
```

**Parameters**

<b>*</b>	Enter the character <code>*</code> to clear all peers.
<b><i>ipv6-address prefix-length</i></b>	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> .

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

<b>dampening</b>	(OPTIONAL) Enter the keyword <code>dampening</code> to clear route flap dampening information.
<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to reset the flap statistics on all prefixes from that neighbor.
<b>peer-group</b>	(OPTIONAL) Enter the keywords <code>peer-group</code> to clear all members of a peer-group.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

**Syntax** `clear ip bgp dampening ipv6 unicast [network network-mask]`

**Parameters**

<b>network</b>	(OPTIONAL) Enter the IPv6 network address in x:x:x:x format.
<b>network-mask</b>	If you enter the network address, next enter the network mask, from 0 to 128.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip bgp ipv6 unicast flap-statistics

Clear BGP flap statistics, which includes the number of flaps and the time of the last flap.

**Syntax** `clear ip bgp ipv6 unicast flap-statistics [network | filter-list list | regexp regexp]`

**Parameters**

<b>network</b>	(OPTIONAL) Enter the IPv6 network address in x:x:x:x format to clear flap statistics.
<b>filter-list list</b>	(OPTIONAL) Enter the keywords <code>filter-list</code> then the name of a configured AS-PATH list (maximum 16 characters).
<b>regexp regexp</b>	(OPTIONAL) Enter the keyword <code>regexp</code> then regular expressions. Use one or a combination of the following: <ul style="list-style-type: none"><li>• . (period) matches on any single character, including white space.</li><li>• * (asterisk) matches on sequences in a pattern (zero or more sequences).</li><li>• + (plus sign) matches on sequences in a pattern (one or more sequences).</li><li>• ? (question mark) matches sequences in a pattern (0 or 1 sequences).</li><li>• [ ] (brackets) matches a range of single-character patterns.</li></ul>

- ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.)
- \$ (dollar sign) matches the end of the output string.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

**Syntax** `debug ip bgp ipv6 unicast dampening`  
 To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

**Parameters** **dampening** Enter the keyword `dampening` to clear route flap dampening information.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the S4820T.

## debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

**Syntax** `debug ip bgp ipv6 unicast peer-group peer-group-name updates [in | out]`  
 To disable debugging, use the `no debug ip bgp ipv6 unicast peer-group peer-group-name updates [in | out]` command.

**Parameters** **peer-group *peer-group-name*** Enter the keywords `peer-group` then the name of the peer-group.

**updates** Enter the keyword `updates` to view BGP update information.

**in** (OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.

**out** (OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.


**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


# debug ip bgp ipv6 unicast updates

View information about BGP updates.

<b>Syntax</b>	debug ip bgp ipv6 unicast <i>ipv6-address prefix-length</i> updates [in   out]	
<b>Parameters</b>	<b><i>ipv6-address</i></b>	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.
	<b><i>prefix-length</i></b>	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b>updates</b>	Enter the keyword updates to view BGP update information.
	<b>in</b>	(OPTIONAL) Enter the keyword in to view only BGP updates received from neighbors.
	<b>out</b>	(OPTIONAL) Enter the keyword out to view only BGP updates sent to neighbors.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# distance bgp

Define an administrative distance for routes.

<b>Syntax</b>	distance bgp <i>external-distance internal-distance local-distance</i>	
	To return to default values, use the no distance bgp command.	
<b>Parameters</b>	<b><i>external-distance</i></b>	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 <b>20</b> .
	<b><i>internal-distance</i></b>	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is <b>200</b> .
	<b><i>local-distance</i></b>	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 <b>200</b> .
<b>Defaults</b>	<ul style="list-style-type: none"><li>external-distance = <b>20</b></li><li>internal-distance = <b>200</b></li><li>local-distance = <b>200</b></li></ul>	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	 <b>CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.</b>	
	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.

## neighbor activate

Allows you to enable a specified neighbor/peer group for the current address and subsequent address family identifier (AFI/SAFI).

**Syntax** `neighbor [ipv6-address | peer-group-name] activate`  
To disable, use the `no neighbor [ipv6-address | peer-group-name] activate` command.

**Parameters**

<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Identify a peer group by name.
<b>activate</b>	Enter the keyword <code>activate</code> to enable the identified neighbor or peer group in the new AFI/SAFI.

**Defaults** Disabled.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using `activate` in the new context, the neighbor/peer group is enabled for AFI/SAFI.


**Related Command** [address family](#) — changes the context to SAFI.

## neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

**Syntax** `neighbor {ipv6-address | peer-group-name} advertisement-interval seconds`  
To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

**Parameters**

<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
<b>seconds</b>	Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is <b>5 seconds</b> for internal BGP peers and <b>30 seconds</b> for external BGP peers.

**Defaults**

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch


Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor default-originate

Inject the default route to a BGP peer or neighbor.

**Syntax** `neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group to set the default route of all routers in that peer group.	
<b>route-map map-name</b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.	

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch


Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor distribute-list

Distribute BGP information using an established prefix list.

**Syntax** `neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group.	
<b>prefix-list-name</b>	Enter the name of an established prefix list. If the prefix list is not configured, the default is <b>permit</b> (to allow all routes).	
<b>in</b>	Enter the keyword <code>in</code> to distribute only inbound traffic.	
<b>out</b>	Enter the keyword <code>out</code> to distribute only outbound traffic.	

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

[neighbor filter-list](#) — assigns a AS-PATH list to a neighbor or peer group.

[neighbor route-map](#) — assigns a route map to a neighbor or peer group.

## neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.


**Syntax**

```
neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]
```

To delete a BGP filter, use the `no neighbor [ipv6-address | peer-group-name] filter-list aspath access-list-name [in | out]` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x::x format.

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

**peer-group-name** Enter the name of the peer group to apply the filter to all routers in the peer group.

**access-list-name** Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is **permit** (to allow routes).

**in** Enter the keyword `in` to filter inbound BGP routes.

**out** Enter the keyword `out` to filter outbound BGP routes.

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor maximum-prefix

Control the number of network prefixes received.


**Syntax**

```
neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x::x format.

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

**peer-group-name** Enter the name of the peer group.

**maximum** Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.

**threshold** (OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is from 1 to 100 percent. The default is **75**.

**warning-only** (OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

**Defaults** threshold = **75**

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.


## neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor.

**Syntax** `neighbor {ipv6-address | peer-group-name} next-hop-self`

To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x:x::x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**peer-group-name** (OPTIONAL) Enter the name of the peer group.

**Defaults** Disabled.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.


## neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

**Syntax** `neighbor {ipv6-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x:x::x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**peer-group-name** Enter the name of the peer group to remove the private AS numbers.

**Defaults** Disabled (that is, the private AS number are not removed).

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY


**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

**Syntax** `neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}`  
To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>peer-group-name</b>	Enter the name of the peer group.	
<b>map-name</b>	Enter the name of an established route map. If the Route map is not configured, the default is <b>deny</b> (to drop all routes).	
<b>in</b>	Enter the keyword <code>in</code> to filter inbound routes.	
<b>out</b>	Enter the keyword <code>out</code> to filter outbound routes.	

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.


**Usage Information** When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

## neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

**Syntax** `neighbor {ipv6-address | peer-group-name} route-reflector-client`  
To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters		
<b>ipv6-address</b>	Enter the IPv6 address in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.

**peer-group-name** Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.


When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

## network

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax** `network ipv6-address [route-map map-name]`  
To remove a network, use the `no network ipv6-address [route-map map-name]` command.

**Parameters**

**ipv6-address** Enter the IPv6 address in the x:x:x:x format.  
 **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

**route-map map-name** (OPTIONAL) Enter the keywords `route-map` then the name of an established route map.  
If the route map is not configured, the default is **deny** (to drop all routes).

**Defaults** Not configured.

**Command Modes** ROUTER BGPV6-ADDRESS FAMILY

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

**Related Commands** [redistribute](#) — redistributes routes into BGP.

## redistribute

Redistribute routes into BGP.

**Syntax** `redistribute {connected | static} [route-map map-name]`  
To disable redistribution, use the `no redistribution {connected | static}` command.

<b>Parameters</b>	<b>connected</b>	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
	<b>static</b>	Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.
	<b>route-map <i>map-name</i></b>	(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 <b>deny</b> (to drop all routes).
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER BGPV6-ADDRESS FAMILY	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>If you do not configure the <code>default-metric</code> command, in addition to the <code>redistribute</code> command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".</p> <p>To redistribute the default route (0::0/0), configure the <code>neighbor default-originate</code> command.</p>	
<b>Related Commands</b>	<code>neighbor default-originate</code> — injects the default route.	

## show ip bgp ipv6 unicast

View the current BGP information.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]</code>	
<b>Parameters</b>	<b>network</b>	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
	<b>network-mask</b>	(OPTIONAL) Enter the keywords <code>network mask</code> (in slash prefix format) of the BGP network address.
	<b>longer-prefixes</b>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	When you enable the <code>bgp non-deterministic-med</code> command, the <code>show ip bgp</code> command output for a BGP route does not list the INACTIVE reason.	

## show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast cluster-list [cluster-id]</code>
---------------	---

**Parameters**      *cluster-id*      (OPTIONAL) Enter the cluster id in dotted decimal format.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast community

View information on all routes with community attributes or view specific BGP community groups.

**Syntax**      `show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]`

<b>Parameters</b>		
<b>community-number</b>		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.
<b>local-AS</b>		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 (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.
<b>no-advertise</b>		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 (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
<b>no-export</b>		Enter the keywords <code>no-export</code> to view 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.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**      To view the total number of COMMUNITY attributes found, use the `show ip bgp ipv6 unicast summary` command. The text line above the route table states the number of COMMUNITY attributes found.

## show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

**Syntax**      `show ip bgp ipv6 unicast community-list community-list-name`

**Parameters**      *community-list-name*      Enter the name of a configured IP community list.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

**Syntax** `show ip bgp ipv6 unicast dampened-paths`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast detail

Display detailed BGP information.

**Syntax** `show ip bgp ipv6 unicast detail`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
R2_Training#show ip bgp ipv6 unicast detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics
327741 :
NhLocAS 1 : NdState 2 : NdRPMPPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal
-1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0
:
NdRRClstTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP
0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRC1P 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP
0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSe
t 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 : NumNhDfrd 0 : CfgHdrAFMsk 1
```



## show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast filter-list <i>as-path-name</i></code>	
<b>Parameters</b>	<b><i>as-path-name</i></b>	Enter the name of an AS-PATH.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

<b>Syntax</b>	<code>show ip bgp ipv6 unicast flap-statistics [<i>ipv6-address prefix-length</i>] [<i>filter-list as-path-name</i>] [<i>regexp regular-expression</i>]</code>	
<b>Parameters</b>	<b><i>ipv6-address prefix-length</i></b>	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.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<b><i>filter-list as-path-name</i></b>	(OPTIONAL) Enter the keywords <i>filter-list</i> then the name of a configured AS-PATH ACL.
	<b><i>regexp regular-expression</i></b>	Enter a regular expression then use one or a combination of the following characters to match: <ul style="list-style-type: none"><li>. = (period) any single character (including a white space).</li><li>* = (asterisk) the sequences in a pattern (0 or more sequences).</li><li>+ = (plus) the sequences in a pattern (1 or more sequences).</li><li>? = (question mark) sequences in a pattern (either 0 or 1 sequences).</li><li> <b>NOTE:</b> You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.</li><li>[ ] = (brackets) a range of single-character patterns.</li><li>^ = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.</li><li>\$ = (dollar sign) the end of the output string.</li></ul>
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ip bgp ipv6 unicast flap-statistics
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, * valid, >
```



```

best Path
source: I - internal, a - aggregate, c - confed-external, r -
redistributed, n -
network Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From           Flaps   Duration  Reuse  Path
h  dead:1::/100     5ffe:10::3    1       00:03:20  1 i
h  dead:1::/100     5ffe:11::3    1       00:03:20  1 i
h  dead:4::/100     5ffe:10::3    1       00:04:39  1 i
h  dead:4::/100     5ffe:11::3    1       00:04:39  1 i

Dell#

```

## show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

**Syntax** `show ip bgp ipv6 unicast inconsistent-as`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

**Syntax** `show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length [advertised-routes | dampened-routes | detail | flap-statistics | routes]]`

Parameters	Description
<b>ipv6-address</b> <b>prefix-length</b>	(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. <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>advertised-routes</b>	(OPTIONAL) Enter the keywords <code>advertised-routes</code> to view only the routes the neighbor sent.
<b>dampened-routes</b>	(OPTIONAL) Enter the keywords <code>dampened-routes</code> to view information on dampened routes from the BGP neighbor.
<b>flap-statistics</b>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to view flap statistics on the neighbor's routes.
<b>detail</b>	(OPTIONAL) Display detailed neighbor information.
<b>routes</b>	(OPTIONAL) Enter the keyword <code>routes</code> to view only the neighbor's feasible routes.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip bgp ipv6 unicast neighbors` command shown in the Example below.

Lines Beginning With	Description
<b>BGP neighbor</b>	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, then the link is internal; otherwise, the link is external.
<b>BGP version</b>	Displays the BGP version (always version 4) and the remote router ID.
<b>BGP state</b>	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
<b>Last read</b>	This line displays the following information: <ul style="list-style-type: none"> <li>last read is the time (hours:minutes:seconds) the router reads a message from its neighbor</li> <li>hold time is the number of seconds configured between messages from its neighbor</li> <li>keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive</li> </ul>
<b>Received messages</b>	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.
<b>Sent messages</b>	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.
<b>Received updates</b>	This line displays the number of BGP updates received and sent.
<b>Minimum time</b>	Displays the minimum time, in seconds, between advertisements.
<b>(List of inbound and outbound policies)</b>	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
<b>For address family:</b>	Displays IPv6 Unicast as the address family.
<b>BGP table version</b>	Displays which version of the primary BGP routing table the router and the neighbor are using.
<b>Accepted Prefixes</b>	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
<b>Prefixes advertised</b>	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
<b>Connections established</b>	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
<b>Last reset</b>	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.
<b>Local host:</b>	Displays the peering address of the local router and the TCP port number.
<b>Foreign host:</b>	Displays the peering address of the neighbor and the TCP port number.

### Example

```
Dell#show ip bgp ipv6 unicast neighbors
```

```

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
  Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

Capabilities advertised to neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 3; dropped 2
Last reset 00:00:39, due to Closed by neighbor

Notification History
  'OPEN error/Bad AS' Sent : 0 Recv: 1

Local host: 5ffe:10::4, Local port: 179
Foreign host: 5ffe:10::3, Foreign port: 35470

Notification History
  'Connection Reset' Sent : 1 Recv: 0

BGP neighbor is 5ffe:11::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:28
  Last read 00:00:28, last write 00:00:28
  Hold time is 180, keepalive interval is 60 seconds
  Received 27 messages, 3 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Received 8 updates, Sent 0 updates
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

Capabilities received from neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)
Capabilities advertised to neighbor for IPv6 Unicast :
  MULTIPROTO_EXT(1)
  ROUTE_REFRESH(2)
  CISCO_ROUTE_REFRESH(128)

For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

Connections established 3; dropped 2
Last reset 00:00:41, due to Closed by neighbor

Notification History

```

```
'OPEN error/Bad AS' Sent : 0 Recv: 1
Local host: 5ffe:11::4, Local port: 179
```

## show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

**Syntax** `show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

**Parameters**

- peer-group-name** (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
- summary** (OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp ipv6 unicast summary` command.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 ipv6 unicast summary

Allows you to view the status of all BGP connections.

**Syntax** `show ip bgp ipv6 unicast summary`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip bgp ipv6 unicast summary` command shown in the Example below.

Field	Description
<b>BGP router identifier</b>	Displays the local router ID and the AS number.
<b>BGP table version</b>	Displays the BGP table version and the main routing table version.
<b>network entries</b>	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
<b>BGP path attribute entries</b>	Displays the number of BGP path attributes and the amount of memory used to process them.

Field	Description
<b>BGP AS-PATH entries</b>	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
<b>BGP community entries</b>	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The <code>show ip bgp ipv6 unicast community</code> command provides more details on the COMMUNITY attributes.
<b>Dampening enabled</b>	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
<b>Neighbor</b>	Displays the BGP neighbor address.
<b>AS</b>	Displays the AS number of the neighbor.
<b>MsgRcvd</b>	Displays the number of BGP messages that neighbor received.
<b>MsgSent</b>	Displays the number of BGP messages that neighbor sent.
<b>TblVer</b>	Displays the version of the BGP table that was sent to that neighbor.
<b>InQ</b>	Displays the number of messages from that neighbor waiting to be processed.
<b>OutQ</b>	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.
<b>Up/Down</b>	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
<b>State/Pfx</b>	<p>If the neighbor is in Established stage, the number of network prefixes received.</p> <p>If a maximum limit was configured with the <code>neighbor maximum-prefix</code> command, (prfxd) appears in this column.</p> <p>If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column.</p> <p>If the neighbor is disabled, the phrase (Admin shut) appears in this column.</p>

### Example

```
Dell#show ip bgp ipv6 unicast summary
BGP router identifier 5.5.10.4, local AS number 100
BGP table version is 12, main routing table version 12
2 network entrie(s) and 4 paths using 536 bytes of memory
1 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths, 0 penalized paths

Neighbor    AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/Pfx
5ffe:10::3  1    28       0        12     0    0 00:01:01  2
5ffe:11::3  1    27       0        12     0    0 00:00:55  2
Dell#
```

# iSCSI Optimization

Internet small computer system interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic on an Aggregator.

**NOTE:** When iSCSI storage devices are detected on the server-ports, storm-control is disabled on those ports. When the iSCSI devices are off the ports, storm-control is enabled again.

## Topics:

- [advertise dcbx-app-tlv](#)
- [iscsi aging time](#)
- [iscsi cos](#)
- [iscsi enable](#)
- [iscsi priority-bits](#)
- [iscsi profile-compellent](#)
- [iscsi target port](#)
- [show iscsi](#)
- [show iscsi sessions](#)
- [show iscsi sessions detailed](#)
- [show run iscsi](#)

## advertise dcbx-app-tlv

Configure DCBX to send iSCSI TLV advertisements.

<b>Syntax</b>	<code>advertise dcbx-app-tlv iscsi</code>
	To disable DCBX iSCSI TLV advertisements, use the <code>no advertise dcbx-app-tlv iscsi</code> command.
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	PROTOCOL LLDP
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can configure iSCSI TLVs to send either globally or on a specified interface. The interface configuration takes priority over global configuration.

## iscsi aging time

Set the aging time for iSCSI sessions.

**Syntax** `iscsi aging time time`

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

**Parameters**      **time**      Enter the aging time for the iSCSI session. The range is from 5 to 43,200 minutes.

**Defaults**      **10 minutes**

**Command Modes**      CONFIGURATION

**Supported Modes**      Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## iscsi cos

Set the QoS policy that is applied to the iSCSI flows.

**Syntax**      `iscsi cos {enable | disable | dot1p vlan-priority-value [remark] | dscp dscp-value [remark]}`

To disable the QoS policy, use the `no iscsi cos dscp` command.

Parameters	enable	disable	dot1p vlan-priority-value	dscp dscp-value	remark
	Enter the keyword <code>enable</code> to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. The default is: the iSCSI packets are handled with dotp1 priority 4 without remark.	Enter the keyword <code>disable</code> to disable the application of preferential QoS treatment to iSCSI frames.	Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The range is from 0 to 7. The default is the dot1p value in ingress iSCSI frames is not changed and is the same priority is used in iSCSI TLV advertisements if you did not enter the <code>iscsi priority-bits</code> command.	Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is from 0 to 63. The default is: the DSCP value in ingress packets is not changed.	Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. The default is: the dot1and DSCP values in egress packets are not changed.

**Defaults**      The default dot1p VLAN priority value is 4 without the `remark` option.

**Command Modes**      CONFIGURATION

**Supported Modes**      Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## iscsi enable

Globally enable iSCSI optimization.

<b>Syntax</b>	<code>iscsi enable</code>	
	To disable iSCSI optimization, use the <code>no iscsi enable</code> command.	
<b>Parameters</b>	<b><i>enable</i></b>	Enter the keyword <code>enable</code> to enable the iSCSI optimization feature.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	9.2(0.0)	Introduced on the M I/O Aggregator.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable the iSCSI feature using the `iscsi enable` command, flow control settings are set to `rx on tx off` on all interfaces.

## iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

<b>Syntax</b>	<code>iscsi priority-bits priority-bitmap</code>	
	To remove the configured iSCSI priority, use the <code>no iscsi priority-bits</code> command.	
<b>Parameters</b>	<b><i>priority-bitmap</i></b>	Enter the priority-bitmap range. The range is from 1 to FF.
<b>Defaults</b>	0x10	
<b>Command Modes</b>	PROTOCOL LLDP	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	9.2(0.0)	Introduced on the M I/O Aggregator.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is available at the global level only.



# iscsi profile-compellent

Configure the auto-detection of Dell Compellent arrays on a port.

- Syntax** `iscsi profile-compellent`
- Defaults** Dell Compellent disk arrays are not detected.
- Command Modes** INTERFACE
- Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# iscsi target port

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication is monitored.

- Syntax** `iscsi target port [tcp-port-2...tcpport-16]ip-address [ip-address]`  
To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.

- Parameters**
  - tcp-port-2...tcpport-16** Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. The default is **860, 3260**.
  - ip-address** (Optional) Enter the ip-address that the iSCSI monitors. The ip-address specifies the IP address of the iSCSI target.

- Defaults** **860, 3260**
- Command Modes** CONFIGURATION

- Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module

**Usage Information** You can configure up to 16 target TCP ports on the switch in one command or multiple commands. When you use the `no iscsi target port` command and the TCP port you wish to delete is one bound to a specific IP address, the IP address value must be included in the command.

# show iscsi

Display the currently configured iSCSI settings.

**Syntax** `show iscsi`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
Dell#show iscsi
iSCSI is enabled
iSCSI session monitoring is enabled
iSCSI COS : dot1p is 4 no-remark
Session aging time: 10
Maximum number of connections is 256
-----
iSCSI Targets and TCP Ports:
-----
TCP Port      Target IP Address
3260
860
Dell#
```

### Related Commands

- [show iscsi sessions](#) — displays information on active iSCSI sessions on the switch that have been established since the last reload.
- [show iscsi sessions detailed](#) — displays detailed information on active iSCSI sessions on the switch.

# show iscsi sessions

Display information on active iSCSI sessions on the switch that have been established since the last reload.

**Syntax** `show iscsi sessions`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
Dell# show iscsi sessions
Session 0:

Target: iqn.2001-05.com.equallogic:0-8a0906-0e70c2002-10a0018426a48c94-
iom010
Initiator: iqn.1991-05.com.microsoft:win-x918v27yajg
ISID: 400001370000

Session 1:
```

```
Target: iqn.2001-05.com.equallogic:0-8a0906-0f60c2002-0360018428d48c94-
iom011
Initiator: iqn.1991-05.com.microsoft:win-x918v27yajg
ISID: 400001370000.
```

- Related Commands**
- [show iscsi](#) — displays the currently configured iSCSI settings.
  - [show iscsi sessions detailed](#) — displays detailed information on active iSCSI sessions on the switch.

## show iscsi sessions detailed

Displays detailed information on active iSCSI sessions on the switch.

**Syntax** `show iscsi sessions detailed [session isid]`

**Parameters**

<b><i>isid</i></b>	Enter the session's iSCSI ID to display detailed information on specified iSCSI session.
--------------------	--

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example**

```
Dell# show iscsi sessions detailed
Session 0 :
-----
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-2c
Up Time:00:00:01:28 (DD:HH:MM:SS)
Time for aging out:00:00:09:34 (DD:HH:MM:SS)
ISID:806978696102
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCPPort ID
10.10.0.44 33345 .10.0.101 3260 0
Session 1 :
-----
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-35
Up Time:00:00:01:22 (DD:HH:MM:SS)
Time for aging out:00:00:09:31 (DD:HH:MM:SS)
ISID:806978696102
Initiator Initiator Target Target Connection
IP Address TCP Port IP Address TCPPort ID
10.10.0.53 33432 10.10.0.101 3260 0
```

- Related Commands**
- [show iscsi](#) — displays the currently configured iSCSI settings.
  - [show iscsi sessions](#) — displays information on active iSCSI sessions on the switch that have been established since the last reload.

## show run iscsi

Display all globally configured non-default iSCSI settings in the current session.

**Syntax** `show run iscsi`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [show iscsi](#) — displays the currently configured iSCSI settings.
- [show iscsi sessions](#) — show iscsi session — displays detailed information about active iSCSI sessions on the switch.
- [show iscsi sessions detailed](#) — displays detailed information on active iSCSI sessions on the switch.

# Intermediate System to Intermediate System (IS-IS)

The Dell Networking OS supports the intermediate system to intermediate system (IS-IS) protocol for IPv4 and IPv6.

IS-IS is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the *Dell Networking OS Configuration Guide*.

**NOTE:** The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

## Topics:

- adjacency-check
- advertise
- area-password
- clear config
- clear isis
- clns host
- debug isis
- debug isis adj-packets
- debug isis local-updates
- debug isis snp-packets
- debug isis spf-triggers
- debug isis update-packets
- default-information originate
- description
- distance
- distribute-list in
- distribute-list out
- distribute-list redistributed-override
- domain-password
- graceful-restart ietf
- graceful-restart interval
- graceful-restart t1
- graceful-restart t2
- graceful-restart t3
- graceful-restart restart-wait
- hello padding
- hostname dynamic
- ignore-lsp-errors
- ip router isis
- ipv6 router isis
- isis circuit-type
- isis csnp-interval
- isis csnp-interval
- isis hello-multiplier

- isis hello padding
- isis ipv6 metric
- isis metric
- isis network point-to-point
- isis password
- isis priority
- is-type
- log-adjacency-changes
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-addresses
- max-lsp-lifetime
- maximum-paths
- metric-style
- multi-topology
- net
- passive-interface
- redistribute
- redistribute bgp
- redistribute ospf
- router isis
- set-overload-bit
- show config
- show isis database
- show isis graceful-restart detail
- show isis hostname
- show isis interface
- show isis neighbors
- show isis protocol
- show isis traffic
- spf-interval

## adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

**Syntax**                    adjacency-check  
                                   To disable adjacency check, use the `no adjacency-check` command.

**Defaults**                 Enabled.

**Command Modes**       • ROUTER ISIS (*for IPv4*)  
                                   • CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

**Supported Modes**      Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**       To perform protocol-support consistency checks on hello packets, use this command. The adjacency-check is enabled by default.

# 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 `level1-into-level2` to advertise Level 1 routes into Level 2 LSPs. This setting is the default.
- level2-into-level1** Enter the keywords `level2-into-level1` to advertise Level 2 inter-area routes into Level 1 LSPs. This behavior is described in RFC 2966.
- prefix-list-name** Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

**Defaults** **level1-into-level2** (Level 1 to Level 2 leaking enabled.)

**Command Modes**

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

You cannot disable leaking from one level to another; however, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all routes are leaked.

You 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 `hmac-md5` to encrypt the password.
- encryption-type** (OPTIONAL) Enter 7 to encrypt the password using DES.
- password** Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.

**Defaults** Not configured.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

**Command  
History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [tag] [* | database | traffic]`

**Parameters**

<b>tag</b>	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*	Enter the keyword * to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.
<b>database</b>	Clears IS-IS LSP database information.
<b>traffic</b>	Clears IS-IS counters.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command  
History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**

<b>name</b>	Enter an alphanumeric string to identify the name-to-NSAP mapping.
<b>nsap</b>	Enter a specific NSAP address that is associated with the name parameter.

**Defaults** Not configured.



**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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 adj-packets [interface]`

To turn off debugging, use the `no debug isis adj-packets [interface]` command.

**Parameters**

***interface***

(OPTIONAL) Identifies the interface type slot/port as one of the following:

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

# debug isis local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

**Syntax** `debug isis local-updates [interface]`  
To turn off debugging, use the `no debug isis local-updates [interface]` command.

**Parameters** *interface* (OPTIONAL) Identifies the interface type slot/port as one of the following:

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

# 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 snp-packets [interface]`  
To turn off debugging, use the `no debug isis snp-packets [interface]` command.

**Parameters** *interface* (OPTIONAL) Identifies the interface type slot/port as one of the following:

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

# debug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

**Syntax** `debug isis spf-triggers`  
To turn off debugging, use the `no debug isis spf-triggers` command.

**Command Modes** EXEC Privilege

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## debug isis update-packets

Enable debugging on link state PDUs (LSPs) that a router detects.

**Syntax** `debug isis update-packets [interface]`  
 To turn off debugging, use the `no debug isis update-packets [interface]` command.

**Parameters**

**interface** (OPTIONAL) Identifies the interface type slot/port as one of the following:

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

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## default-information originate

Generates a default route into an IS-IS routing domain and controls the distribution of default information.

**Syntax** `default-information originate [always] [metric metric] [route-map map-name]`  
 To disable the generation of a default route into the specified IS-IS routing domain, use the `no default-information originate [always] [metric metric] [route-map map-name]` command.

**Parameters**

**always** (OPTIONAL) Enter the keyword `always` to have the default route always advertised.

**metric metric** (OPTIONAL) Enter the keyword `metric` then a number to assign to the route. The range is from 0 to 16777215.

**route-map map-name** (OPTIONAL) A default route the routing process generates if the route map is satisfied.

**Defaults** Not configured.

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.
- [isis metric](#) — configures a metric for an interface.
- [metric-style](#) — sets the metric style for the router.
- [show isis database](#) — displays the IS-IS link state database.

# 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

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

- weight** The administrative distance value indicates the reliability of a routing information source. The range is from 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.) The default is **115**.
- ip-address mask** (OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.
- prefix-list** (OPTIONAL) Enter the name of a prefix list name.

**Defaults** weight = **115**

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>distribute-list <i>prefix-list-name</i> in [<i>interface</i>]</code> To return to the default values, use the <code>no distribute-list <i>prefix-list-name</i> in [<i>interface</i>]</code> command.						
<b>Parameters</b>	<p><b><i>prefix-list-name</i></b> Specify the prefix list to filter prefixes in routing updates.</p> <p><b><i>interface</i></b> (OPTIONAL) Identifies the interface type slot/port as one of the following:</p> <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• ROUTER ISIS (<i>for IPv4</i>)</li> <li>• CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)</li> </ul>						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <a href="#">distribute-list out</a> — suppresses networks from being advertised in updates.</li> <li>• <a href="#">redistribute</a> — redistributes routes from one routing domain to another routing domain.</li> </ul>						

## distribute-list out

Suppress network prefixes from being advertised in outbound updates.

<b>Syntax</b>	<code>distribute-list <i>prefix-list-name</i> out [connected   bgp as <i>number</i>   ospf <i>process-id</i>   rip   static]</code> To return to the default values, use the <code>no distribute-list <i>prefix-list-name</i> out [bgp as <i>number</i> connected   ospf <i>process-id</i>   rip   static]</code> command.
<b>Parameters</b>	<p><b><i>prefix-list-name</i></b> Specify the prefix list to filter prefixes in routing updates.</p> <p><b>connected</b> (OPTIONAL) Enter the keyword <code>connected</code> for directly connected routing process.</p> <p><b>ospf <i>process-id</i></b> (OPTIONAL) Enter the keyword <code>ospf</code> then the OSPF process-ID number. The range is from 1 to 65535.</p> <p><b>bgp as <i>number</i></b> (OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.</p>

- rip** (OPTIONAL) Enter the keyword `rip` for RIP routes.
- static** (OPTIONAL) Enter the keyword `static` for user-configured routing process.

**Defaults** Not configured.

- Command Modes**
- ROUTER ISIS (*for IPv4*)
  - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 `hmac-md5` to encrypt the password using MD5.
  - encryption-type** (OPTIONAL) Enter `7` to encrypt the password using DES.
  - password** Enter an alphanumeric string up to 16 characters long. If you do not specify an `encryption-type` or `hmac-md5` keywords, the password is processed as plain text which provides limited security.

**Defaults** No default password.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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 `ietf` to enable graceful restart on the IS-IS router.

**Defaults**

Graceful restart disabled.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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**

```
graceful-restart interval minutes
```

To return to the default, use the `no graceful-restart interval` command.

**Parameters**

***minutes***

Enter the graceful-restart interval minutes. The range is from 1 to 20 minutes. The default is **5 minutes**.

**Defaults**

**5 minutes**

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 `interval` to set the wait time. The range is from 5 to 120 seconds. The default is **5 seconds**.

**retry-times** Enter the keywords `retry-times` to set the number of times the request interval is extended until a CSNP is received from the helping router. The range is from 1 to 10 attempts. The default is **1**.

**Defaults** Refer to Parameters.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 `level-1` or `level-2` to identify the database instance type to which the wait interval applies.

**seconds** Enter the `graceful-restart t2` time in seconds. The range is from 5 to 120 seconds. The default is **30 seconds**.

**Defaults** **30 seconds**

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.




# graceful-restart t3

Configure the overall wait time before graceful restart completes.

<b>Syntax</b>	<code>graceful-restart t3 {adjacency   manual} seconds</code> To return to the default, use the <code>no graceful-restart t3</code> command.						
<b>Parameters</b>	<table><tr><td><b>adjacency</b></td><td>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.</td></tr><tr><td><b>manual</b></td><td>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 <b>30 seconds</b>.</td></tr></table>	<b>adjacency</b>	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.	<b>manual</b>	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 <b>30 seconds</b> .		
<b>adjacency</b>	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.						
<b>manual</b>	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 <b>30 seconds</b> .						
<b>Defaults</b>	<code>manual</code> , <b>30 seconds</b>						
<b>Command Modes</b>	ROUTER ISIS						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command.</p> <p>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.</p> <p>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>.</p>						
<b>Related Commands</b>	<a href="#">graceful-restart restart-wait</a> — enables the graceful restart maximum wait time before a restarting peer comes up.						

# graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

<b>Syntax</b>	 <b>NOTE:</b> Set the <code>t3</code> timer to <code>adjacency</code> on the restarting router when implementing this command. <code>graceful-restart restart-wait seconds</code> To return to the default, use the <code>no graceful-restart restart-wait</code> command.						
<b>Parameters</b>	<table><tr><td><b>seconds</b></td><td>Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is <b>30 seconds</b>.</td></tr></table>	<b>seconds</b>	Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is <b>30 seconds</b> .				
<b>seconds</b>	Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is <b>30 seconds</b> .						
<b>Defaults</b>	<b>30 seconds</b>						
<b>Command Modes</b>	ROUTER ISIS						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**Related Commands** [graceful-restart t3](#) — configures the overall wait time before graceful restart completes.

## 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** `hello padding [multi-point | point-to-point]`  
To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

**Parameters**

<b>multi-point</b>	(OPTIONAL) Enter the keywords <code>multi-point</code> to pad only LAN hello PDUs.
<b>point-to-point</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To build name-to-systemID mapping tables through the protocol, use this command. All `show` commands that display systems also display the hostname.

**Related Commands** [clns host](#) — defines a name-to-NSAP mapping.

# ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

<b>Syntax</b>	<code>ignore-lsp-errors</code> To return to the default values, use the <code>no ignore-lsp-errors</code> command.						
<b>Defaults</b>	In IS-IS, the default deletes LSPs with internal checksum errors ( <code>no ignore-lsp-errors</code> ).						
<b>Command Modes</b>	ROUTER ISIS						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip router isis [tag]</code> To disable IS-IS on an interface, use the <code>no ip router isis [tag]</code> command.						
<b>Parameters</b>	<table><tr><td><b>tag</b></td><td>(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.</td></tr></table>	<b>tag</b>	(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.				
<b>tag</b>	(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.						
<b>Defaults</b>	No processes are configured.						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	To assign a network entity title to enable IS-IS, use the <code>net</code> command.						
<b>Related Commands</b>	<ul style="list-style-type: none"><li><code>net</code> — configures an IS-IS network entity title (NET) for the routing process.</li><li><code>router isis</code> — enables the IS-IS routing protocol.</li></ul>						

# ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

<b>Syntax</b>	<code>ipv6 router isis [tag]</code> To disable IS-IS routing, use the <code>no router isis [tag]</code> command.
---------------	---

<b>Parameters</b>	<b>tag</b>	(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.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER ISIS	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>Configure a network entity title (the <code>net</code> command) to specify the area address and the router system ID.</p> <p>To establish adjacencies and establish dynamic routing, enable routing on one or more interfaces.</p> <p>You can configure only one IS-IS routing process to perform Level 2 routing. A <code>level-1-2</code> designation performs Level 1 and Level 2 routing at the same time.</p>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <a href="#">net</a> — configures an IS-IS network entity title (NET) for the routing process.</li> <li>• <a href="#">is-type</a> — assigns a type for a given area.</li> </ul>	

## isis circuit-type

Configure the adjacency type on interfaces.

<b>Syntax</b>	<code>isis circuit-type {level-1   level-1-2   level-2-only}</code>	
	To return to the default values, use the <code>no isis circuit-type</code> command.	
<b>Parameters</b>	<b>level-1</b>	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.
	<b>level-1-2</b>	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.
	<b>level-2-only</b>	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.
<b>Defaults</b>	<b>level-1-2</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>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.</p> <p>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.</p>	

# isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

<b>Syntax</b>	<code>isis csnp-interval seconds [level-1   level-2]</code> To return to the default values, use the <code>no isis csnp-interval [seconds] [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>seconds</b>	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 <b>10</b> .
	<b>level-1</b>	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
	<b>level-2</b>	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.
<b>Defaults</b>	seconds = <b>10</b> ; <b>level-1</b> (if not otherwise specified)	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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 csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

<b>Syntax</b>	<code>isis csnp-interval seconds [level-1   level-2]</code> To return to the default values, use the <code>no isis csnp-interval [seconds] [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>seconds</b>	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 <b>10</b> .
	<b>level-1</b>	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
	<b>level-2</b>	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.
<b>Defaults</b>	seconds = <b>10</b> ; <b>level-1</b> (if not otherwise specified)	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

**Syntax** `isis hello-multiplier multiplier [level-1 | level-2]`

To return to the default values, use the `no isis hello-multiplier [multiplier] [level-1 | level-2]` command.

**Parameters**

<b>multiplier</b>	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 <b>3</b> .
<b>level-1</b>	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
<b>level-2</b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>isis ipv6 metric default-metric [level-1   level-2]</code> To return to the default values, use the <code>no ipv6 isis metric [default-metric] [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>default-metric</b>	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 <b>10</b> .
	<b>level-1</b>	(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.
	<b>level-2</b>	(OPTIONAL) Enter the keywords <code>level-2</code> to configure the SPF calculation for Level 2 (inter-area) routing.
<b>Defaults</b>	default-metric = <b>10</b> ; <b>level-1</b> (if not otherwise specified)	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>isis metric default-metric [level-1   level-2]</code> To return to the default values, use the <code>no isis metric [default-metric] [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>default-metric</b>	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 63 for narrow and transition metric styles and from 0 to 16777215 for wide metric styles. The default is <b>10</b> .
	<b>level-1</b>	(OPTIONAL) Enter the keywords <code>level-1</code> to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This setting is the default.
	<b>level-2</b>	(OPTIONAL) Enter the keywords <code>level-2</code> to configure the SPF calculation for Level 2 (inter-area) routing.
<b>Defaults</b>	default-metric = <b>10</b> ; <b>level-1</b> (if not otherwise specified)	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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		
<b>encryption-type</b>	(OPTIONAL)	Enter 7 to encrypt the password using DES.
<b>hmac-md5</b>	(OPTIONAL)	Enter the keywords <code>hmac-md5</code> to encrypt the password using MD5.
<b>password</b>		Assign the interface authentication password.
<b>level-1</b>	(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.
<b>level-2</b>	(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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>isis priority value [level-1   level-2]</code> To return to the default values, use the <code>no isis priority [value] [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>value</b>	This value sets the router priority. The higher the value, the higher the priority. The range is from 0 to 127. The default is <b>64</b> .
	<b>level-1</b>	(OPTIONAL) Specify the priority for Level 1. This setting is the default.
	<b>level-2</b>	(OPTIONAL) Specify the priority for Level 2.
<b>Defaults</b>	value = <b>64</b> ; <b>level-1</b> (if not otherwise specified).	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>is-type {level-1   level-1-2   level-2-only}</code> To return to the default values, use the <code>no is-type</code> command.	
<b>Parameters</b>	<b>level-1</b>	Allows a router to act as a Level 1 router.
	<b>level-1-2</b>	Allows a router to act as both a Level 1 and Level 2 router. This setting is the default.
	<b>level-2-only</b>	Allows a router to act as a Level 2 router.
<b>Defaults</b>	<b>level-1-2</b>	
<b>Command Modes</b>	ROUTER ISIS	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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	Parameter	Description
	<b>level-1</b>	(OPTIONAL) Enter the keywords <code>level-1</code> to apply the configuration to generation of Level-1 LSPs.
	<b>level-2</b>	(OPTIONAL) Enter the keywords <code>level-2</code> to apply the configuration to generation of Level-2 LSPs.
	<b>interval seconds</b>	Enter the maximum number of seconds between LSP generations. The range is from 0 to 120 seconds. The default is <b>5 seconds</b> .
	<b>initial_wait_interval seconds</b>	(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 <b>1 second</b> .
	<b>second_wait_interval seconds</b>	(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 <b>5 seconds</b> .

**Defaults** Refer to *Parameters*.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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 128 to 1497 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is **1497**.

**Defaults** 1497 bytes.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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 has to be less than the seconds value specified with the `max-lsp-lifetime` command. The range is from 1 to 65535 seconds. The default is **900**.

**Defaults** 900 seconds

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.</p> <p>The refresh interval must be less than the LSP lifetime specified with the <code>max-lsp-lifetime</code> 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.</p>						
<b>Related Commands</b>	<a href="#">max-lsp-lifetime</a> — sets the maximum interval that LSPs persist without being refreshed.						

## max-area-addresses

Configure manual area addresses.

<b>Syntax</b>	<code>max-area-addresses number</code>						
	To return to the default values, use the <code>no max-area-addresses</code> command.						
<b>Parameters</b>	<b>number</b>	Set the maximum number of manual area addresses. The range is from 3 to 6. The default is <b>3</b> .					
<b>Defaults</b>	<b>3</b> addresses						
<b>Command Modes</b>	ROUTER ISIS						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>max-lsp-lifetime seconds</code>	
	To restore the default time, use the <code>no max-lsp-lifetime</code> command.	
<b>Parameters</b>	<b>seconds</b>	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 <b>1200</b> .
<b>Defaults</b>	<b>1200</b> seconds	
<b>Command Modes</b>	ROUTER ISIS	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.	
<b>Related Commands</b>	<a href="#">lsp-refresh-interval</a> — 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.

<b>Syntax</b>	<code>maximum-paths number</code>	
	To return to the default values, use the <code>no maximum-paths</code> command.	
<b>Parameters</b>	<b>number</b>	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is from 1 to 16. The default is <b>4</b> .
<b>Defaults</b>	<b>4</b>	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>ROUTER ISIS (<i>for IPv4</i>)</li> <li>CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## metric-style

To generate and accept old-style, new-style, or both styles of type, length, and values (TLV), configure a router.

<b>Syntax</b>	<code>metric-style {narrow [transition]   transition   wide [transition]} [level-1   level-2]</code>	
	To return to the default values, use the <code>no metric-style {narrow [transition]   transition   wide [transition]} [level-1   level-2]</code> command.	
<b>Parameters</b>	<b>narrow</b>	Allows you to generate and accept old-style TLVs. The metric range is from 0 to 63.
	<b>transition</b>	Allows you to generate both old-style and new-style TLVs. The metric range is from 0 to 63.
	<b>wide</b>	Allows you to generate and accept only new-style TLVs. The metric range is from 0 to 16777215.
	<b>level-1</b>	Enables the metric style on Level 1.
	<b>level-2</b>	Enables the metric style on Level 2.
<b>Defaults</b>	<b>narrow</b> ; if no Level is specified, Level-1 and Level-2 are configured.	

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

If you enter the `metric-style wide` command, the system 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.

**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.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

**Supported Modes**

Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes**

Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

# 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 or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 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 information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults** Not configured.

**Command Modes** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

<b>connected</b>	Enter the keyword <code>connected</code> to redistribute active routes into IS-IS.
<b>rip</b>	Enter the keyword <code>rip</code> to redistribute RIP routes into IS-IS.
<b>static</b>	Enter the keyword <code>static</code> to redistribute user-configured routes into IS-IS.
<b>metric metric-value</b>	(OPTIONAL) Assign a value to the redistributed route. The range is from 0 to 16777215. The default is <b>0</b> . Use a value that is consistent with the destination protocol.
<b>metric-type {external   internal}</b>	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following: <ul style="list-style-type: none"><li>• <code>external</code></li><li>• <code>internal</code></li></ul>

- level-1** (OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
- level-1-2** (OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
- level-2** (OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
- route-map *map-name*** (OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routers 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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 system 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 are 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. (New command in Release 6.3.1.)

**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**

<b>AS number</b>	Enter a number that corresponds to the autonomous system number. The range is from 1 to 65355.
<b>level-1</b>	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only.
<b>level-1-2</b>	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
<b>level-2</b>	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This setting is the default.



<b>metric <i>metric-value</i></b>	(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 <b>0</b> .
<b>metric-type {external internal}</b>	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: <ul style="list-style-type: none"> <li>• external</li> <li>• internal</li> </ul>
<b>route-map <i>map-name</i></b>	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)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** BGP to IS-IS redistribution supports “match” options using route maps. You can set the metric value, level, and metric-type of redistributed routes by the redistribution command. You can “set” more advanced options using route maps.

**Example**

```
Dell(conf)#router is
Dell(conf-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type
external route-map rmap-isis-to-bgp
Dell(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external route-map
rmap-isis-to-bgp
```

## redistribute ospf

Redistribute routing information from an OSPF process.

**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**

<b><i>process-id</i></b>	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.
<b>metric <i>metric-value</i></b>	(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 <b>0</b> .
<b>metric-type {external   internal}</b>	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: <ul style="list-style-type: none"> <li>• external</li> <li>• internal</li> </ul>

<b>level-1</b>	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
<b>level-1-2</b>	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
<b>level-2</b>	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
<b>match {external   internal}</b>	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are <ul style="list-style-type: none"> <li>• internal</li> <li>• external</li> </ul>
<b>route-map map-name</b>	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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [tag]`  
 To disable IS-IS routing, use the `no router isis [tag]` command.

**Parameters** **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** ROUTER ISIS

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 its non-pseudonode LSPs, 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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## 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*)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>show isis database [level-1   level-2] [local] [detail   summary] [lspid]</code>	
<b>Parameters</b>	<b>level-1</b>	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
	<b>level-2</b>	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
	<b>local</b>	(OPTIONAL) Displays local link-state database information.
	<b>detail</b>	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
	<b>summary</b>	(OPTIONAL) Summary of link-state database information displays when specified.
	<b>lspid</b>	(OPTIONAL) Display only the specified LSP.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show isis database` command shown in the following example.

<b>Field</b>	<b>Description</b>
<b>IS-IS Level-1/ Level-2 Link State Database</b>	Displays the IS-IS link state database for Level 1 or Level 2.
<b>LSPID</b>	<p>Displays the LSP identifier.</p> <p>The first six octets are the System ID of the originating router.</p> <p>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.</p> <p>The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems.</p>

Field	Description
	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.
<b>LSP Seq Num</b>	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.
<b>LSP Checksum</b>	This is the checksum of the entire LSP packet.
<b>LSP Holdtime</b>	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.
<b>ATT</b>	This value represents the Attach bit. This value indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.
<b>P</b>	This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.
<b>OL</b>	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 graceful-restart detail

Display detailed IS-IS graceful restart related settings.

**Syntax** `show isis graceful-restart detail`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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)
Dell#

```

## show isis hostname

Display IS-IS host names configured or learned on the system.

**Syntax** `show isis hostname`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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 interface [interface]`

**Parameters** *interface* (OPTIONAL) Enter the following keywords and slot/port or number information:

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

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell>show isis int
GigabitEthernet 0/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
GigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

# show isis neighbors

Display information about neighboring (adjacent) routers.

**Syntax** `show isis neighbors [level-1 | level-2] [detail] [interface]`

- Parameters**
- level-1** (OPTIONAL) Displays information about Level 1 IS-IS neighbors.
  - level-2** (OPTIONAL) Displays information about Level 2 IS-IS neighbors.
  - detail** (OPTIONAL) Displays detailed information about neighbors.
  - interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
    - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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
<b>System Id</b>	The value that identifies a system in an area.
<b>Interface</b>	The interface, slot, and port in which the router was discovered.
<b>State</b>	The value providing status about the adjacency state. The range is Up and Init.
<b>Type</b>	This value displays the adjacency type (Layer 2, Layer 2 or both).
<b>Priority</b>	IS-IS priority the neighbor advertises. The neighbor with highest priority becomes the designated router for the interface.
<b>Uptime</b>	Displays the interfaces uptime.
<b>Circuit Id</b>	The neighbor's interpretation of the designated router for the interface.

**Example** The bold sections below identify that Multi-Topology IS-IS is enabled.

```
Dell#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
Dell#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
Topology: IPv4 IPv6 , Common (IPv4 IPv6)
```



## show isis protocol

Display IS-IS routing information.

**Syntax** show isis protocol

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example** The bold section identifies that Multi-Topology IS-IS is enabled.

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
    49.0000.0001
  Routing for area address(es):
    49.0000.0001
  Interfaces supported by IS-IS:
    GigabitEthernet 1/0 - IP - IPv6
    GigabitEthernet 1/1 - IP - IPv6
    GigabitEthernet 1/10 - IP - IPv6
    Loopback 0 - IP - IPv6
  Redistributing:
  Distance: 115
  Generate narrow metrics: level-1-2
  Accept narrow metrics: level-1-2
  Generate wide metrics: none
  Accept wide metrics: none
Multi Topology Routing is enabled in transition mode.
Dell#
```

## show isis traffic

This command allows you to display IS-IS traffic interface information.

**Syntax** show isis traffic [*interface*]

**Parameters** *interface* (OPTIONAL) Identifies the interface type slot/port as one of the following:

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

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show isis traffic` command shown in the following example.

Item	Description
<b>Level-1/Level-2 Hellos (sent/rcvd)</b>	Displays the number of Hello packets sent and received.
<b>PTP Hellos (sent/rcvd)</b>	Displays the number of point-to-point Hellos sent and received.
<b>Level-1/Level-2 LSPs sourced (new/refresh)</b>	Displays the number of new and refreshed LSPs.
<b>Level-1/Level-2 LSPs flooded (sent/rcvd)</b>	Displays the number of flooded LSPs sent and received.
<b>Level-1/Level-2 LSPs CSNPs (sent/rcvd)</b>	Displays the number of CSNP LSPs sent and received.
<b>Level-1/Level-2 LSPs PSNPs (sent/rcvd)</b>	Displays the number of PSNP LSPs sent and received.
<b>Level-1/Level-2 DR Elections</b>	Displays the number of times designated router elections ran.
<b>Level-1/Level-2 SPF Calculations</b>	Displays the number of shortest path first calculations.
<b>LSP checksum errors received</b>	Displays the number of checksum errors LSPs received.
<b>LSP authentication failures</b>	Displays the number of LSP authentication failures.

**Example**

```
Dell#sho 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.

<b>Parameters</b>	<b>level-1</b>	(OPTIONAL) Enter the keyword <code>level-1</code> to apply the configuration to Level-1 SPF calculations.
	<b>level-2</b>	(OPTIONAL) Enter the keyword <code>level-2</code> to apply the configuration to Level-2 SPF calculations.
	<b>interval seconds</b>	Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is <b>10 seconds</b> .
	<b>initial_wait_interval seconds</b>	(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 <b>5 seconds</b> .
	<b>second_wait_interval seconds</b>	(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 <b>5 seconds</b> .

**Defaults** Refer to *Parameters*.

- Command Modes**
- ROUTER ISIS (*for IPv4*)
  - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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).

# Isolated Networks

This chapter describes the isolated networks commands in the Dell Networking OS.

## Topics:

- [io-aggregator isolated-network vlan](#)
- [show io-aggregator isolated-networks](#)

## io-aggregator isolated-network vlan

Enable the isolated-network functionality for a particular VLAN or a set of VLANs.

**Syntax** `[no] io-aggregator isolated-network vlan vlan-range`

<b>Parameters</b>	<b>isolated-network</b>	Specify an isolated network to be configured
	<b>vlan <i>vlan-range</i></b>	Enter the keyword <code>vlan</code> followed by 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** Not configured.

**Command Modes** CONFIGURATION

**Usage Information** To add more VLANs into an isolated network, you can enter this same command at any later point. The VLANs specified are appended to the existing set of VLANs. To remove a VLAN or a set of VLANs from an isolated network, use the `no` form of command.

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.5(0.0)</b>	Supported on the M I/O Aggregator.

## Example

```
Dell(conf)#io-aggregator isolated-network vlan 5-10
```

## show io-aggregator isolated-networks

Display the VLANs that are configured to be part of an isolated network on an Aggregator.

**Syntax** `show io-aggregator isolated-networks`

<b>Parameters</b>	<b>isolated-networks</b>	Specify an isolated network to be configured
	<b>vlan <i>vlan-range</i></b>	Enter the keyword <code>vlan</code> followed by 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** EXEC Privilege

**Usage Information** This command is used to show the isolated-network feature status and the VLANs configured for this feature. Show running-config will save this command under io-aggregator.

**Supported Modes** All Modes

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.5(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.5(0.0)</b>	Supported on the M I/O Aggregator.

**Example**

```
Dell#show io-aggregator isolated-networks
Isolated Network Enabled VLANs : 5-10
```

# Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networking's implementation of the link aggregation control protocol (LACP) for the creation of dynamic link aggregation groups (LAGs — called *port-channels* in Dell Networking OS parlance).

## Topics:

- [auto-lag enable](#)
- [clear lacp counters](#)
- [debug lacp](#)
- [io-aggregator auto-lag enable](#)
- [lacp link-fallback](#)
- [lacp long-timeout](#)
- [lacp port-priority](#)
- [port-channel mode](#)
- [port-channel-protocol lacp](#)
- [show interfaces port-channel](#)
- [show io-aggregator auto-lag status](#)
- [show lacp](#)
- [show link-bundle-distribution port-channel](#)
- [show port-channel-flow](#)

## auto-lag enable

Enable auto-lag on a server facing port.

**Syntax**                    `auto-lag enable`

To disable the auto-lag use the `no auto-lag enable` command.

When disabled, the server port associated in a LAG is removed and the LAG itself gets removed. Any LACPDUs received on the server port are discarded.

**Defaults**                    Enabled

**Command Modes**          INTERFACE

**Supported Modes**        Standalone, Stacking, VLT  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN I/O Aggregator
	<b>9.6(0.0)</b>	Supported on the M I/O Aggregator.

## clear lacp counters

Clear Port Channel counters.

**Syntax**                    `clear lacp port-channel-number counters`

<b>Parameters</b>	<i>port-channel-number</i>	Enter a port-channel number: The range is from 1 to 128.
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Related Commands</b>	<a href="#">show lacp</a> — displays the LACP configuration.	

## debug lacp

Debug LACP (events).

<b>Syntax</b>	<code>debug lacp [pdu interface [in   out]]</code> To disable LACP debugging, use the <code>no debug lacp [pdu interface [in   out]]</code> command.	
<b>Parameters</b>	<b>pdu in   out</b>	(OPTIONAL) Enter the keyword <code>pdu</code> to debug the LACP Protocol Data Unit information. Optionally, enter an <code>in</code> or <code>out</code> parameter to: <ul style="list-style-type: none"> <li>• Receive enter <code>in</code></li> <li>• Transmit enter <code>out</code></li> </ul>
	<b>interface in   out</b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For a Ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li> </ul>
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## io-aggregator auto-lag enable

Enable auto-lag globally on the server facing ports

<b>Syntax</b>	<code>io-aggregator auto-lag enable</code> To disable the auto-lag, use the <code>no io-aggregator auto-lag enable</code> command.  When disabled, all the server ports associated in a LAG are removed and the LAG itself gets removed. Any LACPDU received on the server ports are discarded.
<b>Defaults</b>	Enabled

**Command Modes** CONFIGURATION

**Supported Modes** Standalone, Stacking, VLT  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.6(0.0)</b>	Supported on the M I/O Aggregator.

**Related Commands** [show io-aggregator auto-lag status](#)—displays global information on the auto-lag status.

## lACP link-fallback

Enable the LACP link-fallback feature.

**Syntax** `lACP link-fallback member-independent port-channel 128`  
To disable the LACP link-fallback, use the `no lACP link-fallback member-independent port-channel 128` command.

**Command Modes** INTERFACE  
CONFIGURATION

**Supported Modes** Standalone, Stacking, and VLT  
Full-Switch

**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.

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced the support on VLT mode.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the M I/O Aggregator and FN I/O Aggregator.

## 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)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.

## 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** *priority-value* Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

**Defaults** **32768**

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch

**Command History**




Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## port-channel mode

Configure the LACP port channel mode.

**Syntax** `port-channel number mode [active] [passive] [off]`

**Parameters**

- number* Enter the keywords `number` then a number.
- active** Enter the keyword `active` to set the mode to the active state.  
 **NOTE:** LACP modes are defined in *Usage Information*.
- passive** Enter the keyword `passive` to set the mode to the passive state.  
 **NOTE:** LACP modes are defined in *Usage Information*.
- off** Enter the keyword `off` to set the mode to the off state.  
 **NOTE:** LACP modes are defined in *Usage Information*.

**Defaults** **off**

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	<b>Mode</b>	<b>Function</b>
	<b>active</b>	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
	<b>passive</b>	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets
	<b>off</b>	An interface cannot be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.

## port-channel-protocol lacp

Enable LACP on any LAN port.

**Syntax** `port-channel-protocol lacp`  
To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

### Example

```
Dell(conf)#interface TenGigabitEthernet 0/5
Dell(conf-if-te-0/5)#no shutdown
Dell(conf-if-te-0/5)#port-channel-protocol lacp
Dell(conf-if-te-0/5-lacp)#port-channel 32 mode active
...
Dell(conf)#interface TenGigabitEthernet 0/6
Dell(conf-if-te-0/6)#no shutdown
Dell(conf-if-te-0/6)#port-channel-protocol lacp
Dell(conf-if-te-0/6-lacp)#port-channel 32 mode active
```

# show interfaces port-channel

Display information on configured Port Channel groups.

**Syntax** `show interfaces port-channel [channel-number] [brief|description]`

- Parameters**
- channel-number** For a Port Channel interface, enter the keyword `port-channel` followed by a number. The range is from 1 to 128.
  - brief** (OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.
  - description** (OPTIONAL) Enter the keyword `description` to display interface information with description.

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- For port-channel interfaces, you can specify multiple ports as `port-range`. For example, if you want to display information corresponding to all ports between 1 and 4, specify the port range as `show interfaces port-channel 1 - 4`.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM and added support to display the interface configurations corresponding to a range of ports.
	9.7(0.0)	Introduced on the M I/O Aggregator.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**Usage Information** The following describes the `show interfaces port-channel` command shown in the following example.

Field	Description
<b>Port-Channel 1...</b>	Displays the status of LAG. In the Example, the status of the LAG, LAG fate-sharing group ("Failover-group") is listed.
<b>Hardware is...</b>	Displays the interface's hardware information and its assigned MAC address.
<b>Port-channel is part...</b>	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
<b>Internet address...</b>	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
<b>MTU 1554...</b>	Displays link and IP MTU.
<b>LineSpeed</b>	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
<b>Members in this...</b>	Displays the interfaces belonging to this port channel.
<b>ARP type:...</b>	Displays the ARP type and the ARP timeout value for the interface.
<b>Last clearing...</b>	Displays the time when the <code>show interfaces</code> counters were cleared.
<b>Queueing strategy.</b>	States the packet queuing strategy. FIFO means first in first out.
<b>packets input...</b>	Displays the number of packets and bytes into the interface.
<b>Input 0 IP packets...</b>	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.

Field	Description
<b>0 64-byte...</b>	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
<b>Received 0...</b>	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
<b>Output 0...</b>	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
<b>Rate information...</b>	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
<b>Time since...</b>	Displays the time since the last change in the configuration of this interface.

### Example (EtherScale)

```
Dell#show interfaces port-channel
Port-channel 1 is down, line protocol is down
Hardware address is 00:1e:c9:f1:00:05, Current address is
00:1e:c9:f1:00:05
Interface index is 1107755009
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IP Address Assignment : NONE
DHCP Client-ID :lag1001ec9f10005
MTU 12000 bytes, IP MTU 1500 bytes
LineSpeed auto
Members in this channel:
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 03:28:00
Queueing strategy: fifo
Input Statistics:
0 packets, 0 bytes
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts
0 runts, 0 giants, 0 throttles
0 CRC, 0 overrun, 0 discarded
Output Statistics:
0 packets, 0 bytes, 0 underruns
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts, 0 Unicasts
0 throttles, 0 discarded, 0 collisions
```

**User Information** The following describes the `show interfaces port-channel brief` command shown in the following example.

Field	Description
<b>LAG</b>	Lists the port channel number.
<b>Mode</b>	Lists the mode: <ul style="list-style-type: none"> <li>• L3 — for Layer 3</li> <li>• L2 — for Layer 2</li> </ul>
<b>Status</b>	Displays the status of the port channel. <ul style="list-style-type: none"> <li>• down — if the port channel is disabled (<code>shutdown</code>)</li> <li>• up — if the port channel is enabled (<code>no shutdown</code>)</li> </ul>
<b>Uptime</b>	Displays the age of the port channel in hours:minutes:seconds.
<b>Ports</b>	Lists the interfaces assigned to this port channel.
<b>(untitled)</b>	Displays the status of the physical interfaces (up or down). <ul style="list-style-type: none"> <li>• 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.</li> <li>• In Layer 3 port channels, the primary port is not indicated.</li> </ul>

## Example

```
Dell#show int po bri
Codes: L - LACP Port-channel
       O - OpenFlow Controller Port-channel
       A - Auto Port-channel
       I - Internally Lagged
LAG Mode Status Uptime Ports
L    128 L3 down 00:00:00
Dell#
```

To indicate the LACP fallback, `Internally lagged` is added to the list. When the LAG auto-configures itself, the LAG status describes as 'I'.

## Related Commands

[show lacp](#) — displays the LACP matrix.

# show io-aggregator auto-lag status

Displays global information on the auto-lag status.

**Syntax** `show io-aggregator auto-lag status`

**Command Modes** EXEC

**Supported Modes** Standalone, Stacking, VLT  
Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Supported on the FN I/O Aggregator.
9.6(0.0)	Supported on the M I/O Aggregator.

## Example

```
Dell-ct-mxl-1-b1(conf)#do show io-aggregator auto-lag status
Auto LAG creation on server port(s) is disabled
```

# show lacp

Displays the LACP matrix.

**Syntax** `show lacp port-channel-number [sys-id | counters]`

## Parameters

<b><i>port-channel-number</i></b>	Enter a port-channel number: The range is from 1 to 128.
<b><i>sys-id</i></b>	(OPTIONAL) Enter the keywords <code>sys-id</code> and the value that identifies a system.
<b><i>counters</i></b>	(OPTIONAL) Enter the keyword <code>counters</code> to display the LACP counters.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

Version	Description
8.3.17.0	Supported on the M I/O Aggregator.

**Example  
(Port-Channel-  
Number)**

```
Dell#show lacp 128
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 0/1 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
-----
TenGig 0/1   200   200      0    0         0         0
Dell#
```

**Related  
Commands**

- [clear lacp counters](#) — Clears the LACP counters.
- [show interfaces port-channel](#) — Displays the information on configured Port Channel groups.

## show link-bundle-distribution port-channel

Display the traffic-handling and utilization of the member interfaces of the port channel.

**Syntax** `show link-bundle-distribution port-channel`

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

**Usage Information** The following table describes the output fields of this show command:

Field	Description
<b>Link-bundle trigger threshold</b>	Threshold value that is the checkpoint, exceeding which the link bundle is marked as being overutilized and alarm is generated
<b>LAG bundle number</b>	Number of the LAG bundle
<b>Utilization (In Percent)</b>	Traffic usage in percentage of the packets processed by the port channel
<b>Alarm State</b>	Indicates whether an alarm is generated if overutilization of the port channel occurred. Possible values are Active and Inactive
<b>Interface</b>	Slot and port number, and the type of the member interface of the port channel
<b>Line Protocol</b>	Indicates whether the interface is administratively up or down
<b>Utilization (In Percent)</b>	Traffic usage in percentage of the packets processed by the particular member interface

### Example

```
Dell#show link-bundle-distribution port-channel
Link-bundle trigger threshold - 60

LAG bundle - 1      Utilization[In Percent] - 0      Alarm State -
Inactive

Interface          Line Protocol  Utilization[In Percent]
Te 0/5             Up             0
```

## show port-channel-flow

Display an egress port in a given port-channel flow.

### Syntax

```
show port-channel-flow port-channel number incoming-interface interface
{ src-mac address dest-mac address {vlan vlanid | ether-type }} [ src-ip
address dest-ip address ] [ src-port number dest-port number ]
```

### Parameters

<b>port-channel <i>number</i></b>	Enter the keywords <code>port-channel</code> then the number of the port channel to display flow information. The range is from 1 to 128.
<b>incoming-interface <i>interface</i></b>	Enter the keywords <code>incoming-interface</code> then the interface type and slot/port or number information: <ul style="list-style-type: none"> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>
<b>src-mac <i>address</i></b>	Enter the keywords <code>src-mac</code> then the MAC source address in the <code>nn:nn:nn:nn:nn:nn</code> format.
<b>dest-mac <i>address</i></b>	Enter the keywords <code>dest-mac</code> then the MAC destination address in the <code>nn:nn:nn:nn:nn:nn</code> format.
<b>vlan <i>vlan-id</i></b>	Enter the keyword <code>vlan</code> then the VLAN ID. The range is from 1 to 4094.
<b>ether-type</b>	Enter the keywords <code>ether-type</code> then the ether-value in the <code>XX:XX</code> format.
<b>src-ip <i>address</i></b>	Enter the keywords <code>src-ip</code> then the IP source address in IP address format.
<b>dest-ip <i>address</i></b>	Enter the keywords <code>dest-ip</code> then the IP destination address in IP address format.
<b>src-port <i>number</i></b>	Enter the keywords <code>src-port</code> then the source port number. The range is from 1 to 65536. The default is <b>None</b> .
<b>dest-port <i>number</i></b>	Enter the keywords <code>dest-port</code> then the destination port number. The range is from 1 to 65536. The default is <b>None</b> .

**Command Modes** EXEC

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.


**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.



This chapter describes commands to configure Layer 2 features.

This chapter contains the following sections:

- [MAC Addressing Commands](#)
- [Virtual LAN \(VLAN\) Commands](#)

#### Topics:

- [MAC Addressing Commands](#)
- [Virtual LAN \(VLAN\) Commands](#)

## MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses:

- [clear mac-address-table dynamic](#)
- [mac-address-table aging-time](#)
- [mac-address-table station-move refresh-arp](#)
- [show cam mac stack-unit](#)
- [show mac-address-table](#)

### clear mac-address-table dynamic

Clear the MAC address table of all MAC addresses learned dynamically.

**Syntax** `clear mac-address-table dynamic {address mac-address | all | interface interface | vlan vlan-id}`

<b>Parameters</b>	<b>address <i>mac-address</i></b>	Enter the keyword <code>address</code> followed by a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
	<b>all</b>	Enter the keyword <code>all</code> to delete all MAC address entries in the MAC address table.
	<b>interface <i>interface</i></b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li> </ul>
	<b>vlan <i>vlan-id</i></b>	Enter the keyword <code>vlan</code> followed by a VLAN ID number from 1 to 4094.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

<b>Syntax</b>	<code>mac-address-table aging-time seconds</code> To delete the configured aging time, use the <code>no mac-address-table aging-time seconds</code> command.								
<b>Parameters</b>	<b>seconds</b> Enter either zero (0) or a number as the number of seconds before MAC addresses are released. To disable aging of the MAC address table, enter 0. The range is from 10 to 1000000. The default is <b>1800 seconds</b> .								
<b>Defaults</b>	<b>1800 seconds</b>								
<b>Command Modes</b>	CONFIGURATION								
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch								
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the M I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.								

## mac-address-table static

Associate specific MAC or hardware addresses to an interface and virtual local area networks (VLANs).

<b>Syntax</b>	<code>mac-address-table static mac-address output interface vlan vlan-id</code> To remove a MAC address, use the <code>no mac-address-table static mac-address output interface vlan vlan-id</code> command.						
<b>Parameters</b>	<b>mac-address</b> Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format. <b>output interface</b> Enter the keyword <code>output</code> then one of the following interfaces for which traffic is forwarded: <ul style="list-style-type: none"><li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul> <b>vlan vlan-id</b> Enter the keyword <code>vlan</code> then a VLAN ID number from 1 to 4094.						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						

## 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** Enabled

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Modified the default option from none to Enabled. Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.


**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* [dynamic] [no-station-move | station-move] [sticky]

Parameters		
<b>address_limit</b>		Enter the maximum number of MAC addresses that can be learned on the interface. The range is from 1 to 1000000.
<b>dynamic</b>	(OPTIONAL)	Enter the keyword <code>dynamic</code> to allow aging of MACs even though a learning limit is configured.
<b>no-station-move</b>	(OPTIONAL)	Enter the keywords <code>no-station-move</code> to disallow a station move (associate the learned MAC address with the most recently accessed port) on learned MAC addresses.
<b>station-move</b>	(OPTIONAL)	Enter the keywords <code>station-move</code> to allow a station move on learned MAC addresses.
<b>sticky</b>	(OPTIONAL)	Enter the keyword <code>sticky</code> to allow configuring the sticky mac feature along with the learning limit.

**Defaults** **dynamic**  
 **NOTE:** “Static” means manually entered addresses, which do not age.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

#### Related Commands

[clear counters](#) — Clear counters used in the `show interface` command.

[clear mac-address-table dynamic](#) — clears the MAC address table of all MAC address learned dynamically.

[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.

<b>Syntax</b>	<code>mac learning-limit learn-limit-violation {log   shutdown}</code> To return to the default, use the <code>no mac learning-limit learn-limit-violation {log   shutdown}</code> command.	
<b>Parameters</b>	<b>log</b>	Enter the keyword <code>log</code> to generate a syslog message on a learning-limit violation.
	<b>shutdown</b>	Enter the keyword <code>shutdown</code> to shut down the port on a learning-limit violation.
<b>Defaults</b>	none	
<b>Command Modes</b>	INTERFACE (conf-if-interface-slot/port)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	This command is supported on physical interfaces, static LAGs, and LACP LAGs.	
<b>Related Commands</b>	<a href="#">show mac learning-limit</a> — displays details of the mac learning-limit.	

## mac learning-limit station-move-violation

Specify the actions for a station move violation.

<b>Syntax</b>	<code>mac learning-limit station-move-violation {log   shutdown-both   shutdown-offending   shutdown-original}</code> To disable a configuration, use the <code>no mac learning-limit station-move-violation</code> command, then the configured keyword.
---------------	--

<b>Parameters</b>	<b>log</b>	Enter the keyword <code>log</code> to generate a syslog message on a station move violation.
	<b>shutdown-both</b>	Enter the keyword <code>shutdown</code> to shut down both the original and offending interface and generate a syslog message.
	<b>shutdown-offending</b>	Enter the keywords <code>shutdown-offending</code> to shut down the offending interface and generate a syslog message.
	<b>shutdown-original</b>	Enter the keywords <code>shutdown-original</code> to shut down the original interface and generate a syslog message.
<b>Defaults</b>	none	
<b>Command Modes</b>	INTERFACE (conf-if-interface-slot/port)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	This command is supported on physical interfaces, static LAGs, and LACP LAGs.	
<b>Related Commands</b>	<a href="#">show mac learning-limit</a> — displays details of the mac learning-limit.	

## mac learning-limit reset

Reset the MAC address learning-limit error-disabled state.

<b>Syntax</b>	<code>mac learning-limit reset</code>	
<b>Defaults</b>	none	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>EXEC</li> <li>EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## mac port-security

Enable or disable the port security feature globally in the system.

<b>Syntax</b>	<code>mac port-security</code>	
	To disable the port security, use the <code>no mac port-security</code> command.	
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .	

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, and Z9500.

### Usage Information

Only if you enable the port security, you will be able to configure MAC address learning limit configurations on the interface level.

When you disable the port security, all the interface level configurations are reset. Also, all dynamically learnt MAC addresses on the interfaces configured with MAC address learning limit are cleared.

## show cam mac stack-unit

Display the content addressable memory (CAM) size and the portions allocated for MAC addresses and for MAC ACLs.

**Syntax** `show cam mac stack-unit unit_number port-set port-pipe count [vlan vlan-id] [interface interface]`

### Parameters

<b>stack-unit <i>unit_number</i></b>	(REQUIRED) Enter the keyword <code>stack-unit</code> followed by a stack member number to select the stack unit for which to gather information. The range is 0 to 5.
<b>port-set <i>port-pipe</i></b>	(REQUIRED) Enter the keywords <code>port-set</code> followed by a Port-Pipe number to select the Port-Pipe for which to gather information. The range is 0.
<b>address <i>mac-addr</i></b>	(OPTIONAL) Enter the keyword <code>address</code> followed by a MAC address in the <code>nn:nn:nn:nn:nn:nn</code> format to display information on that MAC address.
<b>dynamic</b>	(OPTIONAL) Enter the keyword <code>dynamic</code> to display only those MAC addresses learned dynamically by the switch.
<b>static</b>	(OPTIONAL) Enter the keyword <code>static</code> to display only those MAC address specifically configured on the switch.
<b>interface <i>interface</i></b>	(OPTIONAL) Enter the keyword <code>interface</code> followed by the interface type, slot and port information: <ul style="list-style-type: none"> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> followed by the slot/port information.</li> </ul>
<b>vlan <i>vlan-id</i></b>	(OPTIONAL) Enter the keyword <code>vlan</code> followed by the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

## show mac-address-table

Display the MAC address table.

**Syntax** `show mac-address-table [dynamic | static] [address mac-address | interface interface | vlan vlan-id] [count [vlan vlan-id] [interface interface-type [slot [/port]]]]`

<b>Parameters</b>	<b>dynamic</b>	(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/mac-address</code> , <code>interface/interface</code> , or <code>vlan vlan-id</code> .
	<b>static</b>	(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/mac-address</code> , <code>interface/interface</code> , or <code>vlan vlan-id</code> .
	<b>address mac-address</b>	(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.
	<b>interface interface</b>	(OPTIONAL) Enter the keyword <code>interface</code> then the interface type, slot and port information: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>
	<b>interface interface-type</b>	(OPTIONAL) Instead of entering the keyword <code>interface</code> then the interface type, slot and port information, as above, you can enter the interface type, then just a slot number.
	<b>vlan vlan-id</b>	(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.
	<b>count</b>	(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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information** The following describes the `show mac-address-table` command shown in the following example.

<b>Column Heading</b>	<b>Description</b>
<b>VlanId</b>	Displays the VLAN ID number.
<b>Mac Address</b>	Displays the MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<b>Type</b>	Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).
<b>Interface</b>	Displays the interface type and slot/port information. The following abbreviations describe the interface types: <ul style="list-style-type: none"> <li>• gi — Gigabit Ethernet then a slot/port.</li> <li>• po — Port Channel then a number. The range is from 1 to 255 for TeraScale.</li> <li>• so — SONET then a slot/port.</li> <li>• te — 10 Gigabit Ethernet then a slot/port.</li> </ul>
<b>State</b>	Lists if the MAC address is in use (Active) or not in use (Inactive).

## Example

```
Dell#show mac-address-table
VlanId Mac Address      Type      Interface  State
20      00:00:c9:ad:f6:12 Dynamic Te 0/3     Active
Dell#
```

## Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
<b>VlanId</b>	Displays the VLAN ID number.
<b>Mac Address</b>	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
<b>Type</b>	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.
<b>Interface</b>	Displays the interface type and slot/port information. The following abbreviations describe the interface types: <ul style="list-style-type: none"><li>• gi — Gigabit Ethernet then a slot/port</li><li>• po — Port Channel then a number. The range is from 1 to 255. \</li><li>• so — SONET then a slot/port.</li><li>• te — 10-Gigabit Ethernet then a slot/port.</li></ul>
<b>State</b>	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
<b>MAC Entries...</b>	Displays the number of MAC entries learned per VLAN.
<b>Dynamic Address...</b>	Lists the number of dynamically learned MAC addresses.
<b>Static Address...</b>	Lists the number of user-defined MAC addresses.
<b>Total MAC...</b>	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 :      5
Static Address (User-defined) Count : 0
Total MAC Addresses in Use:      5
Dell#
```

## show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

<b>Syntax</b>	<code>show mac-address-table aging-time [vlan <i>vlan-id</i>]</code>
<b>Parameters</b>	<b>vlan <i>vlan-id</i></b> (OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>• EXEC</li><li>• EXEC Privilege</li></ul>
<b>Supported Modes</b>	Full-Switch



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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 `violate-action` to display the MAC learning limit violation status.
- detail** (OPTIONAL) Enter the keyword `detail` to display the MAC learning limit in detail.
- interface *interface*** (OPTIONAL) Enter the keyword `interface` with the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#show mac learning-limit
Interface Learning Dynamic Static Unknown SA
Slot/port Limit MAC count MAC count Drops
Dell#
```

## Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual local area networks (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

For more information, also refer to [Virtual LAN \(VLAN\) Commands](#).

## description

Add a description about the selected VLAN.

**Syntax** `description description`

To remove the description from the VLAN, use the `no description` command.

**Parameters** **description** Enter a text string description to identify the VLAN (80 characters maximum).

**Defaults** none

**Command Modes** INTERFACE VLAN

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Related Commands** [show vlan](#) – displays the VLAN configuration.

## default vlan-id

Specify a VLAN as the Default VLAN.

**Syntax** `default vlan-id vlan-id`

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id vlan-id` syntax.

**Parameters** **vlan-id** Enter the VLAN ID number of the VLAN to become the new Default VLAN. The range is from 1 to 4094. The default is **1**.

**Defaults** The Default VLAN is VLAN **1**.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To return VLAN 1 as the Default VLAN, use the `(default-vlan-id 1)` command. The Default VLAN contains only untagged interfaces.

**Related Commands** [interface vlan](#) — configures a VLAN.

## default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

**Defaults** Enabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**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**

[description](#) — assigns a descriptive text string to the interface.

[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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-if-vl-100)#show config
!
interface Vlan 1
  description a
  no ip address
  mtu 2500
```

```
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 `brief` to display the following information:

- VLAN ID
- VLAN name (left blank if none is configured)
- Spanning Tree Group ID
- MAC address aging time
- IP address

**id *vlan-id*** (OPTIONAL) Enter the keyword `id` then a number from 1 to 4094. Only information on the VLAN specified is displayed.

**name *vlan-name*** (OPTIONAL) Enter the keyword `name` then the name configured for the VLAN. Only information on the VLAN named is displayed.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show vlan` command shown in the following example.

Column Heading	Description
<b>(Column 1 — no heading)</b>	<ul style="list-style-type: none"><li>• asterisk symbol (*) = Default VLAN</li><li>• G = GVRP VLAN</li><li>• P = primary VLAN</li><li>• C = community VLAN</li><li>• I = isolated VLAN</li><li>• O = OpenFlow</li></ul>
<b>NUM</b>	Displays existing VLAN IDs.
<b>Status</b>	Displays the word <i>Inactive</i> for inactive VLANs and the word <i>Active</i> for active VLANs.
<b>Q</b>	<ul style="list-style-type: none"><li>• Displays G for GVRP tagged</li><li>• M for member of a VLAN-Stack VLAN</li><li>• T for tagged interface</li><li>• U for untagged interface</li><li>• x (not capitalized x) for Dot1x untagged</li><li>• X (capitalized X) for Dot1x tagged</li><li>• o (not capitalized o) for OpenFlow untagged</li><li>• O (capitalized O) for OpenFlow tagged</li><li>• H for VSN tagged</li><li>• i (not capitalized i) for Internal untagged</li><li>• I (capitalized I) for Internal tagged</li></ul>

**Column Heading****Description**

- v (not capitalized v) for VLT untagged
- V (capitalized V) for VLT tagged

**Ports**

Displays the type, slot, and port information.

- Po = port channel
- Gi = gigabit Ethernet
- Te = ten-gigabit Ethernet

**Example**

```
Dell#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring
VLANs, P -
Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT
tagged
   NUM  Status  Description  Q  Ports
   1    Inactive  a
   2    Inactive
*  20   Active           U Te 0/3,5,13,53-56
  1002 Active           T Te 0/3,13,55-56
Dell#
```

**Example (VLAN ID)**

```
Dell# show vlan id 40

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring
VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack, H - VSN tagged
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V
- VLT tagged
   NUM  Status  Description  Q  Ports
   1    Inactive  a
Dell#
```

**Example (Brief)**

```
Dell#show vlan brief
VLAN Name STG MAC Aging IP Address
-----
1          0  0          unassigned
2          0  0          unassigned
20         0  0          unassigned
1002       0  0          unassigned
Dell#
```

**Example (Name)**

```
Dellconf)#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 Gi 1/22
Dell(conf-if-vl-222)#
```

**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 or number information:

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

**Defaults** All interfaces in Layer 2 mode are untagged.

**Command Modes** INTERFACE VLAN

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

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

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

**Defaults** Not configured.

**Command Modes** INTERFACE VLAN

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 or number information:

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

**Defaults**

All interfaces in Layer 2 mode are untagged.

**Command Modes**

INTERFACE VLAN

**Supported Modes**

Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

# 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. LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking OS implementation of LLDP is based on IEEE standard 801.1ab.

This chapter describes the LLDP commands.

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).

For details about implementing LLDP/LLDP-MED, refer to the Link Layer Discovery Protocol chapter of the *Dell PowerEdge FN I/O Aggregator Configuration Guide*.

## Topics:

- [advertise dot1-tlv](#)
- [advertise dot3-tlv](#)
- [advertise interface-port-desc](#)
- [advertise management-tlv](#)
- [clear lldp counters](#)
- [clear lldp neighbors](#)
- [debug lldp interface](#)
- [disable](#)
- [hello](#)
- [mode](#)
- [multiplier](#)
- [protocol lldp \(Configuration\)](#)
- [protocol lldp \(Interface\)](#)
- [show lldp neighbors](#)
- [show lldp statistics](#)
- [show running-config lldp](#)
- [LLDP-MED 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**

<b>port-protocol-vlan-id</b>	Enter the keywords <code>port-protocol-vlan-id</code> to advertise the port protocol VLAN identification TLV.
<b>port-vlan-id</b>	Enter the keywords <code>port-vlan-id</code> to advertise the port VLAN identification TLV.
<b>vlan-name</b>	Enter the keywords <code>vlan-name</code> to advertise the vlan-name TLV.

**Defaults** Disabled.



**Command Modes** CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [protocol lldp \(Configuration\)](#) — enables LLDP globally.
- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

## advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

**Syntax** `advertise dot3-tlv {max-frame-size}`  
To remove advertised dot3-tlv, use the `no advertise dot3-tlv {max-frame-size}` command.

**Parameters** **max-frame-size** Enter the keywords `max-frame-size` to advertise the dot3 maximum frame size.

**Defaults** none

**Command Modes** CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## advertise interface-port-desc

Advertise port descriptor.

**Syntax** `advertise interface-port-desc {description | port-id}`  
To remove the advertised port descriptor, use the `no advertise interface-port-desc {description | port-id}` command.

**Parameters** **description** Enter the keyword `description` then the interface description.  
**port-id** Enter the keyword `port-id` then the port-id. The range is from 0 to 7.

**Defaults** None

**Command Modes** CONFIGURATION (conf-lldp)  
INTERFACE (conf-if-*interface*-lldp)

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

Version	Description
9.11(2.0P1)	Introduced the <code>description</code> and <code>port-id</code> options.

**Usage Information** If you do not specify the option, by default the `port-id` takes higher precedence and sends the `port-id` in the LLDP packets.

## advertise management-tlv

Advertise management TLVs (Type, Length, Value).

**Syntax** `advertise management-tlv {system-capabilities | system-description | system-name}`

To remove advertised management TLVs, use the `no advertise management-tlv {system-capabilities | system-description | system-name}` command.

Parameters		
<b>system-capabilities</b>	Enter the keywords <code>system-capabilities</code> to advertise the system capabilities TLVs to the LLDP peer.	
<b>system-description</b>	Enter the keywords <code>system-description</code> to advertise the system description TLVs to the LLDP peer.	
<b>system-name</b>	Enter the keywords <code>system-name</code> to advertise the system name TLVs to the LLDP peer.	

**Defaults** none

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.16.1	Introduced on the M I/O Aggregator.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The command options `system-capabilities`, `system-description`, and `system-name` can be invoked individually or together, in any sequence.

## 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 or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` followed by the slot/port information.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## 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 or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## debug lldp interface

Enable LLDP debugging to display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets.

**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**

<i>interface</i>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>For a 10-Gigabit Ethernet interface, enter the keyword <code>tenGigabitEthernet</code> followed by the slot/port information.</li></ul>
<b>all</b>	(OPTIONAL) Enter the keyword <code>all</code> to display information on all interfaces.
<b>events</b>	(OPTIONAL) Enter the keyword <code>events</code> to display major events such as timer events.
<b>packet</b>	(OPTIONAL) Enter the keyword <code>packet</code> to display information regarding packets coming in or going out.
<b>brief</b>	(OPTIONAL) Enter the keyword <code>brief</code> to display brief packet information.
<b>detail</b>	(OPTIONAL) Enter the keyword <code>detail</code> to display detailed packet information.
<b>tx</b>	(OPTIONAL) Enter the keyword <code>tx</code> to display transmit-only packet information.
<b>rx</b>	(OPTIONAL) Enter the keyword <code>rx</code> to display receive-only packet information.

	<b>both</b>	(OPTIONAL) Enter the keyword <code>both</code> to display both receive and transmit packet information.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## disable

Enable or disable LLDP.

<b>Syntax</b>	<code>disable</code>	
	To enable LLDP, use the <code>no disable</code> command.	
<b>Defaults</b>	Enabled, that is <code>no disable</code> .	
<b>Command Modes</b>	CONFIGURATION ( <code>conf-ldp</code> ) and INTERFACE ( <code>conf-if-interface-ldp</code> )	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Related Commands

## hello

Configure the rate at which the LLDP control packets are sent to its peer.

<b>Syntax</b>	<code>hello seconds</code>	
	To revert to the default, use the <code>no hello seconds</code> command.	
<b>Parameters</b>	<b>seconds</b>	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 <b>30 seconds</b> .
<b>Defaults</b>	<b>30 seconds</b>	
<b>Command Modes</b>	CONFIGURATION ( <code>conf-ldp</code> ) and INTERFACE ( <code>conf-if-interface-ldp</code> )	
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## mode

To receive or transmit, set LLDP.

**Syntax** `mode {tx | rx}`  
 To return to the default, use the `no mode {tx | rx}` command.

**Parameters**

<b>tx</b>	Enter the keyword <code>tx</code> to set the mode to transmit.
<b>rx</b>	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`)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `multiplier integer`  
 To return to the default, use the `no multiplier integer` command.

**Parameters**

<b>integer</b>	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`)

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

Version	Description
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## protocol lldp (Configuration)

Enable LLDP globally on the switch.

**Syntax** `protocol lldp`  
 To disable LLDP globally on the chassis, use the `no protocol lldp` command.

**Defaults** Enabled.

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

## protocol lldp (Interface)

Enter the LLDP protocol in the INTERFACE mode.

**Syntax** `[no] protocol lldp`  
 To return to the global LLDP configuration mode, use the `no protocol lldp` command from Interface mode.

**Defaults** Enabled

**Command Modes** INTERFACE (conf-if-interface-lldp)

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information** This command is available only in PMUX mode.

By default, protocol lldp is enabled, To disable, use the `no protocol lldp` command.

When you enter the LLDP protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

# show lldp neighbors

Display LLDP neighbor information for all interfaces or a specified interface.

- Syntax** `show lldp neighbors [interface] [detail]`
- Parameters**
- interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - detail** (OPTIONAL) Enter the keyword `detail` to display all the TLV information, timers, and LLDP tx and rx counters.

- Defaults** none
- Command Modes** EXEC Privilege
- Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**Usage Information** Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and host name.

**Example**

```
Dell (conf-if-te-0/3)#do show lldp neighbors
Loc PortID  Rem Host Name  Rem Port Id      Rem Chassis Id
-----
Te 0/1      FTOS           TenGigabitEthernet 0/5  00:01:e8:05:40:46
Te 0/2      FTOS           TenGigabitEthernet 0/6  00:01:e8:05:40:46
Te 0/3      FTOS           TenGigabitEthernet 0/7  00:01:e8:05:40:46
Dell (conf-if-te-0/3)#
```

# show lldp statistics

Displays the LLDP statistical information.

- Syntax** `show lldp statistics`
- Defaults** none
- Command Modes** EXEC Privilege
- Supported Modes** All Modes
- Command History**
- | Version  | Description                         |
|----------|-------------------------------------|
| 9.9(0.0) | Introduced on the FN IOM.           |
| 9.4(0.0) | Supported on the FN I/O Aggregator. |
| 8.3.17.0 | Supported on the M I/O Aggregator.  |

**Example**

```
Dell#show lldp statistics
----- LLDP GLOBAL STATISTICS ON CHASSIS -----
Total number of neighbors: 4
Last table change time: 00:01:17, In ticks: 3859
Total number of Table Inserts: 7
Total number of Table Deletes: 3
Total number of Table Drops: 0
Total number of Table Age Outs: 0
Dell#
```

# show running-config lldp

Display the current global LLDP configuration.

<b>Syntax</b>	show running-config lldp
<b>Defaults</b>	none
<b>Command Modes</b>	EXEC Privilege
<b>Supported Modes</b>	Full-Switch
<b>Command History</b>	<b>9.9(0.0)</b> Introduced on the FN IOM. <b>Version 8.3.16.1</b> Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show running-config lldp
!
protocol lldp
  advertise dot1-tlv port-protocol-vlan-id port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-capabilities system-description
  hello 15
  multiplier 3
  no disable
Dell#
```

# LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

The LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands.

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.

<b>Syntax</b>	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.

<b>Parameters</b>	<b>vlan-id</b> Enter the VLAN ID. The range is from 1 to 4094.
	<b>layer2_priority</b> Enter the Layer 2 priority. The range is from 0 to 7.



***DSCP\_value*** Enter the DSCP value. The range is from 0 to 63.

***priority-tagged number*** Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is from 0 to 7.

**Defaults** Unconfigured.

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** Full-Switch

**Command History**

**9.9(0.0)** Introduced on the FN IOM.

**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

[protocol lldp \(Configuration\)](#) — enables LLDP globally.

[debug lldp interface](#) — debugs LLDP.

[show lldp neighbors](#) — displays the LLDP neighbors.

[show running-config lldp](#) — displays the LLDP running configuration.

## advertise med guest-voice-signaling

To advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data, configure the system.

**Syntax** `advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

**Parameters**

***vlan-id*** Enter the VLAN ID. The range is from 1 to 4094.

***layer2\_priority*** Enter the Layer 2 priority. The range is from 0 to 7.

***DSCP\_value*** Enter the DSCP value. The range is from 0 to 63.

***priority-tagged number*** Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

**Defaults** unconfigured.

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** Full-Switch

**Command History**

**9.9(0.0)** Introduced on the FN IOM.

**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

[debug lldp interface](#) — debugs LLDP.

[show lldp neighbors](#) — displays the LLDP neighbors.

[show running-config lldp](#) — displays the LLDP running configuration.

## advertise med location-identification

To advertise a location identifier, configure the system.

**Syntax** `advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}`

To return to the default, use the `no advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}` command.

#### Parameters

- coordinate-based value** Enter the keywords `coordinate-based` then the coordinated based location in hexadecimal value of 16 bytes.
- civic-based value** Enter the keywords `civic-based` then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
- ecs-elin value** Enter the keywords `ecs-elin` then the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is from 10 to 25 characters.

**Defaults** unconfigured.

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** Full-Switch

**Command History** **9.9(0.0)** Introduced on the FN IOM.

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

- ECS — Emergency call service such as defined by TIA or the national emergency numbering association (NENA)
- ELIN — Emergency location identification number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

#### Related Commands

- [debug lldp interface](#) — debugs LLDP.
- [show lldp neighbors](#) — displays the LLDP neighbors.
- [show running-config lldp](#) — displays the LLDP running configuration.

## advertise med power-via-mdi

To advertise the Extended Power via MDI TLV, configure the system.

**Syntax** `advertise med power-via-mdi`

To return to the default, use the `no advertise med power-via-mdi` command.

**Defaults** unconfigured.

**Command Modes** CONFIGURATION (conf-lldp)

**Supported Modes** Full-Switch

**Command History** **9.9(0.0)** Introduced on the FN IOM.

**Version 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.
- [show running-config lldp](#) — displays the LLDP running configuration.

## advertise med softphone-voice

To advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone, configure the system.

<b>Syntax</b>	<code>advertise med softphone-voice {vlan-id}   {priority-tagged number}</code> To return to the default, use the <code>no advertise med softphone-voice {vlan-id}   {priority-tagged number}</code> command.				
<b>Parameters</b>	<table><tr><td><b><i>vlan-id</i></b></td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td><b><i>priority-tagged number</i></b></td><td>Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.</td></tr></table>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.	<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.				
<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.				
<b>Defaults</b>	unconfigured.				
<b>Command Modes</b>	CONFIGURATION (conf-lldp)				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	<p><b>9.9(0.0)</b> Introduced on the FN IOM.</p> <p><b>Version 8.3.16.1</b> Introduced on the MXL 10/40GbE Switch IO Module.</p>				
<b>Related Commands</b>	<p><a href="#">debug lldp interface</a> — debugs LLDP.</p> <p><a href="#">show lldp neighbors</a> — displays the LLDP neighbors.</p> <p><a href="#">show running-config lldp</a> — displays the LLDP running configuration.</p>				

## 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.

<b>Syntax</b>	<code>advertise med streaming-video {vlan-id}   {priority-tagged number}</code> To return to the default, use the <code>no advertise med streaming-video {vlan-id}   {priority-tagged number}</code> command.				
<b>Parameters</b>	<table><tr><td><b><i>vlan-id</i></b></td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td><b><i>priority-tagged number</i></b></td><td>Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.</td></tr></table>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.	<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.				
<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.				
<b>Defaults</b>	unconfigured.				
<b>Command Modes</b>	CONFIGURATION (conf-lldp)				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	<p><b>9.9(0.0)</b> Introduced on the FN IOM.</p> <p><b>Version 8.3.16.1</b> Introduced on the MXL 10/40GbE Switch IO Module.</p>				
<b>Related Commands</b>	<p><a href="#">debug lldp interface</a> — debugs LLDP.</p> <p><a href="#">show lldp neighbors</a> — displays the LLDP neighbors.</p> <p><a href="#">show running-config lldp</a> — displays the LLDP running configuration.</p>				

## advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

<b>Syntax</b>	<code>advertise med video-conferencing {<i>vlan-id</i>}   {priority-tagged <i>number</i>}</code> To return to the default, use the <code>no advertise med video-conferencing {<i>vlan-id</i>}   {priority-tagged <i>number</i>}</code> command.				
<b>Parameters</b>	<table><tr><td><b><i>vlan-id</i></b></td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td><b>priority-tagged <i>number</i></b></td><td>Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.</td></tr></table>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.	<b>priority-tagged <i>number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.				
<b>priority-tagged <i>number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.				
<b>Defaults</b>	unconfigured.				
<b>Command Modes</b>	CONFIGURATION (conf-lldp)				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	<table><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>Version 8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></table>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>9.9(0.0)</b>	Introduced on the FN IOM.				
<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.				
<b>Related Commands</b>	<p><a href="#">debug lldp interface</a> — debugs LLDP.</p> <p><a href="#">show lldp neighbors</a> — displays the LLDP neighbors.</p> <p><a href="#">show running-config lldp</a> — displays the LLDP running configuration.</p>				

## advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

<b>Syntax</b>	<code>advertise med voice-signaling {<i>vlan-id</i>}   {priority-tagged <i>number</i>}</code> To return to the default, use the <code>no advertise med voice-signaling {<i>vlan-id</i>}   {priority-tagged <i>number</i>}</code> command.				
<b>Parameters</b>	<table><tr><td><b><i>vlan-id</i></b></td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td><b>priority-tagged <i>number</i></b></td><td>Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.</td></tr></table>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.	<b>priority-tagged <i>number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.				
<b>priority-tagged <i>number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.				
<b>Defaults</b>	unconfigured.				
<b>Command Modes</b>	CONFIGURATION (conf-lldp)				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	<table><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>Version 8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></table>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>9.9(0.0)</b>	Introduced on the FN IOM.				
<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.				
<b>Related Commands</b>	<p><a href="#">debug lldp interface</a> — debugs LLDP.</p> <p><a href="#">show lldp neighbors</a> — displays the LLDP neighbors.</p> <p><a href="#">show running-config lldp</a> — displays the LLDP running configuration.</p>				

## advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

<b>Syntax</b>	<code>advertise med voice {<i>vlan-id</i>}   {priority-tagged <i>number</i>}</code>
---------------	---

To return to the default, use the `no advertise med voice {vlan-id} | {priority-tagged number}` command.

<b>Parameters</b>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.
	<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b>Defaults</b>	unconfigured.	
<b>Command Modes</b>	CONFIGURATION (conf-lldp)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">debug lldp interface</a> — debugs LLDP.	
	<a href="#">show lldp neighbors</a> — displays the LLDP neighbors.	
	<a href="#">show running-config lldp</a> — displays the LLDP running configuration.	

## advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

<b>Syntax</b>	<code>advertise med voice-signaling {vlan-id}   {priority-tagged number}</code>	
	To return to the default, use the <code>no advertise med voice-signaling {vlan-id}   {priority-tagged number}</code> command.	
<b>Parameters</b>	<b><i>vlan-id</i></b>	Enter the VLAN ID. The range is from 1 to 4094.
	<b><i>priority-tagged number</i></b>	Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
<b>Defaults</b>	unconfigured.	
<b>Command Modes</b>	CONFIGURATION (conf-lldp)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>Version 8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">debug lldp interface</a> — debugs LLDP.	
	<a href="#">show lldp neighbors</a> — displays the LLDP neighbors.	
	<a href="#">show running-config lldp</a> — displays the LLDP running configuration.	

# 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. NLB uses a distributed methodology or pattern to equally split and balance the network traffic load across a set of servers that are part of the cluster or group. NLB combines the servers into a single multicast group and attempts to use the standard multicast IP or unicast IP addresses, and MAC addresses for the transmission of network traffic. At the same time, it also uses a single virtual IP address for all clients as the destination IP address, which enables servers to join the same multicast group in a way that is transparent to the clients (the clients do not notice the addition of new servers to the group). The clients use a cluster IP address to connect to the server. The NLB functionality enables flooding of traffic over the VLAN ports (for unicast mode) or a subset of ports in a VLAN (for multicast mode) to avoid overloading and effective performance of the servers for optimal processing of data packets. The maximum NLB entry limit from 8 to 11 is increased and support for more CAM-ACL to increase.

NLB functions in two modes, namely unicast mode and multicast mode. The cluster IP address and the associated cluster MAC address are configured in the NLB application running on the Windows Server. In the unicast mode, when the server IP address is attempted to be resolved to the MAC address using the ARP application, the switch determines whether the ARP reply, obtained from the server, is of an NLB type. The switch then maps the IP address (cluster IP) with the MAC address (cluster MAC address). In multicast mode, the cluster IP address is mapped to a cluster multicast MAC address that is configured using a static ARP CLI configuration command. After the NLB entry is learned, the traffic is forwarded to all the servers in the VLAN corresponding to the cluster virtual IP address.

## NLB Unicast Mode Scenario

Consider a sample topology in which four servers, namely S1 through S4, are configured as a cluster or a farm. This set of servers is connected to a Layer 3 switch, which in turn is connected to the end-clients. The servers contain a single IP address (IP-cluster address of 172.16.2.20) and a single unicast MAC address (MAC-Cluster address of 00-bf-ac-10-00-01) for load-balancing. Because multiple ports of a switch cannot learn a single MAC address, the servers are assigned with MAC addresses of MAC-s1 to MAC-s4) respectively on S1 through S4 in addition to the MAC cluster address. All the servers of the cluster belong to the VLAN named VLAN1.

In unicast NLB mode, the following sequence of events occurs:

- The switch sends an ARP request to resolve the IP address to the cluster MAC address.
- The ARP servers send an ARP response with the MAC cluster address in the ARP header and a MAC address of MAC-s1/s2/s3/s4 (for servers S1 through S4) in the Ethernet header.
- The switch associates the IP address with the MAC cluster address with the last ARP response it obtains. Assume that in this case, the last ARP reply is obtained from MAC-s4.(assuming that the ARP response with MAC-s4 is received as the last one). The interface associated with server, S4, is added to the ARP table.
- With NLB feature enabled, after learning the NLB ARP entry, all the subsequent traffic is flooded on all ports in VLAN1.

With NLB, the data frame is forwarded to all the servers for them to perform load-balancing.

## NLB Multicast Mode Scenario

Consider a sample topology in which four servers, namely S1 through S4, are configured as a cluster or a farm. This set of servers is connected to a Layer 3 switch, which in turn is connected to the end-clients. They contain a single multicast MAC address (MAC-Cluster: 03-00-5E-11-11-11).

In the multicast NLB mode, a static ARP configuration command is configured to associate the cluster IP address with a multicast cluster MAC address.

With multicast NLB mode, the data is forwarded to all the servers based on the port specified using the Layer 2 multicast command, which is the `mac-address-table static <multicast_mac> multicast vlan <vlan_id> output-range <port1>, <port2>` command in CONFIGURATION mode.

# Limitations With Enabling NLB on Switches

The following limitations apply to switches on which you configure NLB:

- The NLB unicast mode uses switch flooding to transmit all packets to all the servers that are part of the VLAN. When a large volume of traffic is processed, the clustering performance might be impacted in a small way. This limitation is applicable to switches that perform unicast flooding in the software.
- The `ip vlan-flooding` command applies globally across the system and for all VLANs. In cases where the NLB is applicable and the ARP replies contain a discrepancy in the Ethernet SHA and ARP header SHA frames, a flooding of packets over the relevant VLAN occurs.
- The maximum number of concurrent clusters that is supported is 128.

# Benefits and Working of Microsoft Clustering

Microsoft clustering allows multiple servers using Microsoft Windows to be represented by one MAC address and IP address in order to provide transparent failover or balancing. Dell Networking OS does not recognize server clusters by default; it must be configured to do so. When an ARP request is sent to a server cluster, either the active server or all the servers send a reply, depending on the cluster configuration. If the active server sends a reply, the Dell switch learns the active server's MAC address. If all servers reply, the switch registers only the last received ARP reply, and the switch learns one server's actual MAC address; the virtual MAC address is never learned. Because the virtual MAC address is never learned, traffic is forwarded to only one server rather than the entire cluster, and failover and balancing are not preserved.

To preserve failover and balancing, the switch forwards the traffic destined for the server cluster to all member ports in the VLAN connected to the cluster. To ensure that this happens, you must configure the `ip vlan-flooding` command on the Dell switch at the time that the Microsoft cluster is configured. The server MAC address is given in the Ethernet frame header of the ARP reply, while the virtual MAC address representing the cluster is given in the payload. Then, all the traffic destined for the cluster is flooded out of all member ports. Since all the servers in the cluster receive traffic, failover and balancing are preserved.

# Enable and Disable VLAN Flooding

- The older ARP entries are overwritten whenever newer NLB entries are learned.
- All ARP entries, learned after the feature is enabled, are deleted when the feature is disabled, and RP2 triggers an ARP resolution. The feature is disabled with the `no ip vlan-flooding` command.
- When a port is added to the VLAN, the port automatically receives traffic if the feature is enabled. Old ARP entries are not deleted or updated.
- When a member port is deleted, its ARP entries are also deleted from the CAM.
- Port channels in the VLAN also receive traffic.
- There is no impact on the configuration from saving the configuration.
- The feature, if enabled, is displayed in the `show running-config` command output that displays the `ip vlan-flooding` CLI configuration. Apart from it, there is no indication of the enabling of this capability.

## Topics:

- [mac-address-table static \(for Multicast MAC Address\)](#)
- [ip vlan-flooding](#)


# 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**

- multicast-mac-address** Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
- multicast** Enter a vlan port to where L2 multicast MAC traffic is forwarded.  
 **NOTE:** Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.
- output interface** For a multicast MAC address, enter the keyword `output` then one of the following interfaces for which traffic is forwarded:
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- output-range interface** For a multicast MAC address, enter the keyword `output-range` then one of the following interfaces to indicate a range of ports for which traffic is forwarded:
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- vlan vlan-id** Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	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 0/2,Te 0/3}`

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.3(0.0)	Introduced on the MXL Switch .

**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.

## Topics:

- [clear ip msdp peer](#)
- [clear ip msdp sa-cache](#)
- [clear ip msdp statistic](#)
- [debug ip msdp](#)
- [ip msdp cache-rejected-sa](#)
- [ip msdp default-peer](#)
- [ip msdp log-adjacency-changes](#)
- [ip msdp mesh-group](#)
- [ip msdp originator-id](#)
- [ip msdp peer](#)
- [ip msdp redistribute](#)
- [ip msdp sa-filter](#)
- [ip msdp sa-limit](#)
- [ip msdp shutdown](#)
- [ip multicast-msdp](#)
- [show ip msdp](#)
- [show ip msdp sa-cache rejected-sa](#)

## clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL Switch .

## 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]`

<b>Parameters</b>	<b><i>group-address</i></b>	Enter the group IP address in dotted decimal format (A.B.C.D.).
	<b><i>rejected-sa</i></b>	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.
	<b><i>local</i></b>	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.
<b>Defaults</b>	Without any options, this command clears the entire source-active cache.	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL Switch .

## 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.

<b>Syntax</b>	<code>clear ip msdp sa-cache [<i>group-address</i>   <i>rejected-sa</i>   <i>local</i>]</code>	
<b>Parameters</b>	<b><i>group-address</i></b>	Enter the group IP address in dotted decimal format (A.B.C.D.).
	<b><i>rejected-sa</i></b>	Enter the keyword <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.
	<b><i>local</i></b>	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.
<b>Defaults</b>	Without any options, this command clears the entire source-active cache.	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## debug ip msdp

Turn on MSDP debugging.

<b>Syntax</b>	<code>debug ip msdp {event <i>peer address</i>   packet <i>peer address</i>   pim}</code>	
	To turn debugging off, use the <code>no debug ip msdp {event <i>peer address</i>   packet <i>peer address</i>   pim}</code> command.	
<b>Parameters</b>	<b><i>event peer address</i></b>	Enter the keyword <code>event</code> then the peer address in a dotted decimal format (A.B.C.D.).

<b>packet <i>peer address</i></b>	Enter the keyword <code>packet</code> then the peer address in a dotted decimal format (A.B.C.D.).
<b>pim</b>	Enter the keyword <code>pim</code> to debug advertisement from PIM.

**Defaults** Not configured.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Version 9.2(0.0)** Introduced on the MXL 10/40GbE Switch IO Module.

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>9.2(0.0)</b>	Introduced on the MXL Switch .

**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** ***peer address*** Enter the peer address in a dotted decimal format (A.B.C.D.)  
***list name*** Enter the keywords `list name` and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `ip msdp log-adjacency-changes`  
To disable logging, use the `no ip msdp log-adjacency-changes` command.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip msdp mesh-group

To be a member of a mesh group, configure a peer.

**Syntax** `ip msdp mesh-group {name} {peer address}`  
To remove the peer from a mesh group, use the `no ip msdp mesh-group {name} {peer address}` command.

**Parameters**

<b><i>name</i></b>	Enter a string of up to 16 characters long for as the mesh group name.
<b><i>peer address</i></b>	Enter the peer address in a dotted decimal format (A.B.C.D.).

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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 information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

# 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**

**peer address** Enter the peer address in a dotted decimal format (A.B.C.D.).

**connect-source interface** Enter the keywords `connect-source` then one of the interfaces and slot/port or number information:

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

**description name** (OPTIONAL) Enter the keyword `description` then a description name (maximum 80 characters) to designate a description for the MSDP peer.

**sa-limit number** (OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000. The default is **500000**.

**Defaults** As described in the *Parameters* section.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>ip msdp redistribute [list <i>acl-name</i>]</code>	
<b>Parameters</b>	<b>list <i>acl-name</i></b>	Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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 <code>clear ip msdp sa-cache local</code> command.	

## ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

<b>Syntax</b>	<code>ip msdp sa-filter {in   out} <i>peer-address</i> list [<i>access-list name</i>]</code>	
	Remove this configuration using the <code>no ip msdp sa-filter {in   out} <i>peer address</i> list [<i>access-list name</i>]</code> command.	
<b>Parameters</b>	<b>in</b>	Enter the keyword <code>in</code> to enable incoming SA filtering.
	<b>out</b>	Enter the keyword <code>out</code> to enable outgoing SA filtering.
	<b><i>peer-address</i></b>	Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
	<b><i>access-list name</i></b>	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  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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** *number* Enter the maximum number of SA entries in SA-cache. The range is from 0 to 40000.

**Defaults** 50000

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system counts the SA messages originated by itself and those messages received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in the software 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** `ip msdp shutdown {peer address}`

**Parameters** *peer address* Enter the peer address in a dotted decimal format (A.B.C.D.).

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch



<b>Command History</b>	<b>Version</b>	<b>Version</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip multicast-msdp

Enable MSDP.

**Syntax** `ip multicast-msdp`  
To exit MSDP, use the `no ip multicast-msdp` command.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 peer address** Enter the keyword `peer` then the peer address in a dotted decimal format (A.B.C.D.).
- sa-cache** Enter the keywords `sa-cache` to display the Source-Active cache.
- summary** Enter the keyword `summary` to display an MSDP peer summary.

**Defaults** Not configured.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#sh 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
Dell#
```

# Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking Operating System (OS), conforms to IEEE 802.1s.

## Topics:

- [debug spanning-tree mstp](#)
- [description](#)
- [disable](#)
- [disable](#)
- [forward-delay](#)
- [hello-time](#)
- [max-age](#)
- [max-hops](#)
- [msti](#)
- [name](#)
- [port-channel path-cost custom](#)
- [protocol spanning-tree mstp](#)
- [revision](#)
- [show config](#)
- [show spanning-tree mst configuration](#)
- [show spanning-tree msti](#)
- [spanning-tree](#)
- [spanning-tree msti](#)
- [spanning-tree mstp](#)
- [tc-flush-standard](#)

## 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]`

<b>Parameters</b>	<b>all</b>	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
	<b>bpdu <i>interface</i> {in   out}</b>	(OPTIONAL) Enter the keyword <code>bpdu</code> 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: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul> Optionally, enter an <code>in</code> or <code>out</code> parameter with the optional interface: <ul style="list-style-type: none"> <li>• For Receive, enter the keyword <code>in</code>.</li> <li>• For Transmit, enter the keyword <code>out</code>.</li> </ul>
	<b>events</b>	(OPTIONAL) Enter the keyword <code>events</code> to debug MSTP events.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#debug spanning-tree mstp bpdu tengigabitethernet 0/16 ?
in Receive (in)
out Transmit (out)
Dell#
```

## description

Enter a description of the multiple spanning tree.

**Syntax** `description {description}`  
 To remove the description, use the `no description {description}` command.

**Parameters** *description* Enter a description to identify the multiple spanning tree (maximum 80 characters).

**Defaults** none

**Command Modes** SPANNING TREE (The prompt is “config-mstp”.)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [protocol spanning-tree mstp](#) — enters MULTIPLE SPANNING TREE mode on the switch.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [protocol spanning-tree mstp](#) — enters MULTIPLE SPANNING TREE mode.

# disable

Enable bridge protocol data units (BPDU) filter globally to filter transmission of BPDU on port-fast enabled interfaces.

**Syntax** `edge-port bpdufilter default`  
To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.

**Defaults** disabled.

**Command Modes** MULTIPLE SPANNING TREE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on MXL 10/40GbE Switch IO Module

# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [edge-port bpdufilter default](#) — 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** *max-age* Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

**Defaults** **20 seconds**

**Command Modes** MULTIPLE SPANNING TREE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [edge-port bpdufilter default](#) — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.  
[hello-time](#) — changes the time interval between BPDUs.

## max-hops

Configure the maximum hop count.

**Syntax** `max-hops number`  
To return to the default values, use the `no max-hops` command.

**Parameters** *range* Enter a number for the maximum hop count. The range is from 1 to 40. The default is **20**.

**Defaults** **20 hops**

**Command Modes** MULTIPLE SPANNING TREE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The `max-hops` command is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reach zero, the switch discards the BPDU and ages out any information that it holds for the port.

## msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

### Syntax

```
msti instance {vlan range | bridge-priority priority}
```

To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

### Parameters

<b>msti <i>instance</i></b>	Enter the MSTP instance. The range is from zero (0) to 63.
<b>vlan <i>range</i></b>	Enter the keyword <code>vlan</code> then the identifier range value. The range is from 1 to 4094.
<b>bridge-priority <i>priority</i></b>	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

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

Although MSTP instance IDs range from 0 to 4094, only 64 active instances are supported on the switch.

## 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

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## port-channel path-cost custom

Sets the path cost to be constant for port-channel regardless of its operation status.

**Syntax** `port-channel path-cost custom`  
 To change the path cost to comply with new IEEE standard behavior, use `no port-channel path-cost custom` command.

**Defaults** Disabled

**Command Modes** SPANNING TREE

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

Version	Description
9.13(0.1)	Introduced on MXL, FN IOM, S6000, S3100, S4810, S4820T, S3048-ON, S4048-ON, S4048T-ON, S6000-ON, S6010-ON, S6100-ON, S5048F-ON, C9010, and Z9100-ON,

**Usage Information**

This command is used to keep the port-channel path cost constant regardless of the operational status of the port-channel member ports.

This command is supported in all STP modes such as STP, RSTP, MSTP, and PVST.

The command behavior does not change when a new member port is added to the port-channel or an existing member port is deleted from the configuration. The path cost reflects the cumulative speed of the port-channel member ports.

**Example**

```
DELEMC(conf)#protocol spanning-tree pvst
DELEMC(conf-pvst)#port-channel path-cost custom
```

## 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.



**Usage Information** MSTP is not enabled when you enter MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter the `no disable` command while in MULTIPLE SPANNING TREE mode.

For more information about the multiple spanning tree protocol, refer to the *Dell Networking OS Configuration Guide*.

**Example**

```
Dell(conf)#protocol spanning-tree mstp
Dell(config-mstp)#no disable
```

**Related Commands** `disable` — disables multiple spanning tree.

## revision

The revision number for the multiple spanning tree configuration.

**Syntax** `revision range`  
To return to the default values, use the `no revision` command.

**Parameters** *range* Enter the revision number for the MST configuration. The range is from 0 to 65535. The default is **0**.

**Defaults** **0**

**Command Modes** MULTIPLE SPANNING TREE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `show config`

**Command Modes** MULTIPLE SPANNING TREE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-mstp)#show config
!
protocol spanning-tree mstp
no disable
name CustomerSvc
```

```
revision 2
MSTI 10 VLAN 101-105
max-hops 5
Dell(conf-mstp)#
```

## show spanning-tree mst configuration

View the multiple spanning tree configuration.

**Syntax** `show spanning-tree mst configuration`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**
- instance-number*** (Optional) Enter the multiple spanning tree instance number. The range is from 0 to 63.
  - brief** (Optional) Enter the keyword `brief` to view a synopsis of the MST instance.
  - guard** (Optional) Enter the keyword `guard` to display the type of guard enabled on an MSTP interface and the current port state.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Enable the multiple spanning tree protocol prior to using this command.

### Example

```
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.e800.0204
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 0001.e800.0204
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
Bpdu filter disabled globally
CIST regional root ID Priority 32768, Address 0001.e800.0204
CIST external path cost 0

```

Interface Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
Te 0/10	128.170	128	2000	FWD	0	32768 0001.e800.0204	128.170
Te 0/11	128.171	128	2000	FWD	0	32768 0001.e800.0204	128.171
Te 0/12	128.172	128	2000	FWD	0	32768 0001.e800.0204	128.172

```

Interface Bpdu
Name Role PortID Prio Cost Sts Cost Link-type Edge Filter
Boundary
-----
Te 0/10 Desg 128.170 128 2000 FWD 0 P2P No No
No
Te 0/11 Desg 128.171 128 2000 FWD 0 P2P No No
No
Te 0/12 Desg 128.172 128 2000 FWD 0 P2P No No
No
Dell#

```

**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
-----
Gi 0/0 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257

Interface
Name Role PortID Prio Cost Sts Cost Link-type Edge Boundary
-----
Gi 0/0 ErrDis 128.257 128 20000 EDS 0 P2P No No

Dell#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occurred 00:00:15 ago on Gi 0/0

Port 257 (GigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8

```

```
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

### Usage Information

The following describes the `show spanning-tree msti 5 guard` command shown in the following example.

Field	Description
<b>Interface Name</b>	MSTP interface.
<b>Instance</b>	MSTP instance.
<b>Sts</b>	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
<b>Guard Type</b>	Type of STP guard configured (Root, Loop, or BPDU guard).

### Example (Guard)

```
Dell#show spanning-tree msti 0 guard
Executing IEEE compatible Spanning Tree Protocol
Bpdu filter disabled globally

Interface
Name      Instance Sts  Guard type  Bpdu Filter
-----
Te 0/10   0        FWD   None       No
Te 0/11   0        FWD   None       No
Te 0/12   0        FWD   None       No
```

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 `msti` and the MST instance number. The range is from zero (0) to 63.
- cost cost** (OPTIONAL) Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are:

- 10-Gigabit Ethernet interface = **2000**
- Port Channel interface with one 10 Gigabit Ethernet = **2000**
- Port Channel with two 10 Gigabit Ethernet = **1800**
- Port Channel with two 100 Mbps Ethernet = **180000**

**priority *priority*** Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.

**Defaults**

- cost = depends on the interface type
- priority = **128**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## spanning-tree mstp

Configures a Layer 2 MSTP interface as an edge port with (optionally) a bridge protocol data unit (BPDU) guard, or enables the root guard or loop guard feature on the interface.

**Syntax** `spanning-tree mstp {edge-port [bpduguard [shutdown-on-violation]] | bpdufilter| rootguard}`

**Parameters**

<b>edge-port</b>	Enter the keywords <code>edge-port</code> to configure the interface as a multiple spanning tree edge port.
<b>bpduguard</b>	(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.
<b>bpdufilter</b>	(OPTIONAL) Enter the keyword <code>edgeport</code> to enable edge port configuration to move the interface into forwarding mode immediately after the root fails. Enter the keyword <code>bpdufilter</code> to stop sending and receiving BPDUs on the port-fast enabled ports.
<b>shutdown-on-violation</b>	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
<b>rootguard</b>	Enter the keyword <code>rootguard</code> to enable root guard on an MSTP port or port-channel interface.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

On an MSTP switch, a port configured as an edge port 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 `spanning-tree portfast` enabled.

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.`

When used in an MSTP network, if root guard blocks a boundary port in the CIST, the port is also blocked in all other MST instances.

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.

## 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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

By default, the system implements an optimized flush mechanism for MSTP. This mechanism helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this `knob` command can be turned on to enable flushing MAC addresses after receiving every topology change notification.

# Multicast

The multicast commands are supported by Dell Networking Operating System (OS).

This chapter contains the following sections:

- [IPv4 Multicast Commands](#)
- [IPv6 Multicast Commands](#)

## Topics:

- [IPv4 Multicast Commands](#)
- [clear ip mroute](#)
- [ip mroute](#)
- [ip multicast-limit](#)
- [ip multicast-routing](#)
- [mtrace](#)
- [show ip mroute](#)
- [show ip rpf](#)
- [IPv6 Multicast Commands](#)
- [debug ipv6 mld\\_host](#)
- [ip multicast-limit](#)

## 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** `clear ip mroute {group-address [source-address] | * | snooping}`

**Parameters**

<b><i>group-address</i></b>	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
<b>[<i>source-address</i>]</b>	
*	Enter * to clear all multicast routes.
<b>snooping</b>	Enter the keyword <code>snooping</code> to delete multicast snooping route table entries.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2.(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [show ip pim tib](#) — shows the PIM tree information base.

# ip mroute

Assign a static mroute.

**Syntax** `ip mroute destination mask {ip-address | null 0} {{bgp| ospf} process-id | isis | rip | static} {ip-address | tag | null 0} [distance]`

To delete a specific static mroute, use the `ip mroute destination mask {ip-address | null 0} {{bgp| ospf} process-id | isis | rip | static} {ip-address | tag | null 0} [distance]` command.

To delete all mroutes matching a certain mroute, use the `no ip mroute destination mask` command.

**Parameters**

- destination** Enter the IP address in dotted decimal format of the destination device.
- mask** Enter the mask in slash prefix formation ( /x ) or in dotted decimal format.
- null 0** (OPTIONAL) Enter the keyword `null` then zero (0).
- [protocol [process-id | tag] ip-address]** (OPTIONAL) Enter one of the routing protocols:
  - Enter the BGP as-number then the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is from 1 to 65535.
  - Enter the OSPF process identification number then the IP address in dotted decimal format of the RPF neighbor. the range is from 1 to 65535.
  - Enter the IS-IS alphanumeric tag string then the IP address in dotted decimal format of the RPF neighbor.
  - Enter the RIP IP address in dotted decimal format of the RPF neighbor.
- static ip-address** (OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
- ip-address** (OPTIONAL) Enter the IP address in dotted decimal format of the RPF neighbor.
- distance** (OPTIONAL) Enter a number as the distance metric assigned to the mroute. The range is from 0 to 255.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [show ip mroute](#) — views the multicast routing table.

# ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

**Syntax** `ip multicast-limit limit`

**Parameters**

- limit** Enter the desired maximum number of multicast entries on the system. The range is from 1 to 50000.

**Defaults** 15000 routes.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch



<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>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.</p> <p>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 <code>ip multicast-limit</code> command is reached.</p>						

## ip multicast-routing

Enable IP multicast forwarding.

**Syntax** `ip multicast-routing`

To disable multicast forwarding, use the `no ip multicast-routing` command.

**Defaults** Disabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**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.

## mtrace

Trace a multicast route from the source to the receiver.

**Syntax** `mtrace [vrf vrf-name] {source-address/hostname} [destination-address/hostname] [group-address/hostname]`

<b>Parameters</b>	<p><b>vrf vrf-name</b> Enter the keyword <code>vrf</code> followed by the name of the VRF. If VRF name is not mentioned, the default VRF will be used. Mtrace is not supported for management VRF.</p> <p><b>source-address/hostname</b> Enter the source IP address in dotted decimal format (A.B.C.D). This is a unicast address of the beginning of the path to be traced.</p> <p><b>destination-address/hostname</b> Enter the destination (receiver) IP address in dotted decimal format (A.B.C.D). If omitted, the mtrace starts from the system at which the command is typed.</p> <p><b>group-address/hostnaae</b> Enter the multicast group address in dotted decimal format (A.B.C.D). If group address is not given then software shall invokes a weak mtrace. A weak mtrace is one that follows the RPF path to the source, regardless of whether any router along the path has multicast routing table state</p>
-------------------	---

**Command Modes** EXEC Privilege

**Command History**

Version	Description
9.11.0.0	Re-introduced the mtrace command on the Dell EMC Networking OS.
7.5.1.0	Expanded to support originator.
7.4.1.0	Expanded to support the intermediate (transit) router.

**Usage Information**

Mtrace is an IGMP based protocol that provides a multicast trace route facility and is implemented according to the IETF draft "A *trace route* facility for IP Multicast" (draft-fenner-traceroute-ipm-01.txt). Dell EMC Networking OS supports the Mtrace client and transit functionality.

As an Mtrace client, Dell EMC Networking OS transmits Mtrace queries, receives, parses, and prints out the details in the response packet received.

A transit or intermediate router, forwards mtrace requests to the RPF neighbor after appending its response block to the packet. In case it is the first hop router, it sends a response.

As an Mtrace transit or intermediate router, Dell EMC Networking OS returns the response to Mtrace queries. After receiving the Mtrace request, Dell EMC Networking OS computes the RPF neighbor for the source, fills in the request and the forwards the request to the RPF neighbor.

**Example**

```
R1>mtrace 103.103.103.3 1.1.1.1 226.0.0.3
Type Ctrl-C to abort.

Querying reverse path for source 103.103.103.3 to destination 1.1.1.1
via group 226.0.0.3
From source (?) to destination (?)

-----
|Hop|      OIF IP          |Proto| Forwarding Code |Source Network/Mask|
-----
  0  1.1.1.1            -->  Destination
 -1  1.1.1.1            PIM   Reached RP/Core  103.103.103.0/24
 -2  101.101.101.102   PIM   -                103.103.103.0/24
 -3  2.2.2.1            PIM   -                103.103.103.0/24
 -4  103.103.103.3     -->  Source
-----
```

The mtrace command traverses the path of the response data block in the reverse direction of the multicast data traffic. The mtrace command traverses the reverse path to the source from the destination. As a result, the tabular output of the mtrace command displays the destination details in the first row, followed by the RPF router details along the path in the consequent rows, and finally the source details in the last row. The tabular output contains the following columns:

- Hop — a hop number(counted negatively to indicate reverse-path)
- OIF IP — outgoing interface address
- Proto — multicast routing protocol
- Forwarding code — error code as present in the response blocks
- Source Network/Mask — source mask

## show ip mroute

View the multicast routing table.

**Syntax**

```
show ip mroute [static | group-address [source-address] | count | snooping
[vlan vlan-id] [group-address [source-address]] | summary | vlt [group-
address [source-address] | count]
```

**Parameters**

- static** (OPTIONAL) Enter the keyword *static* to view static multicast routes.
- group-address [source-address]** (OPTIONAL) Enter the multicast group-address to view only routes associated with that group.

Enter the source-address to view routes with that group-address and source-address.

**count** (OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.

**snooping [vlan vlan-id] [group-address [source-address]]** Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers.

Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094.

Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.

**summary** (OPTIONAL) Enter the keyword `summary` to view a summary of all routes.

**vlt** (OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2.(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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
(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 0/4
    TenGigabitEthernet 1/5
(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 0/3
    TenGigabitEthernet 0/4
    TenGigabitEthernet 0/5
```

**Example**

```
Dell#show ip mroute
```

```

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 0/2
  Outgoing interface list:
    TenGigabitEthernet 0/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: TenGigabitEthernet 1/4
  Outgoing interface list:
    TenGigabitEthernet 0/6
    TenGigabitEthernet 0/7

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 1/2
  Outgoing interface list:
    TenGigabitEthernet 1/4

```

### Usage Information

The following describes the `show ip mroute` command shown in the following example.

Field	Description
<b>(S, G)</b>	Displays the forwarding entry in the multicast route table.
<b>uptime</b>	Displays the amount of time the entry has been in the multicast forwarding table.
<b>Incoming interface</b>	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
<b>Outgoing interface list:</b>	Lists the interfaces that meet one of the following: <ul style="list-style-type: none"> <li>• a directly connected member of the Group</li> <li>• statically configured member of the Group</li> <li>• received a (*,G) or (S,G) Join message</li> </ul>

### Example

```

Dell#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 1/2
  Outgoing interface list:
    TenGigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: TenGigabitEthernet 1/4
  Outgoing interface list:
    TenGigabitEthernet 0/2
    TenGigabitEthernet 0/3


(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 1/2
  Outgoing interface list:
    TenGigabitEthernet 1/4

```

## show ip rpf

View reverse path forwarding.

- Syntax** `show ip rpf`
- Command Modes**
- EXEC
  - EXEC Privilege
- Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2.(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2.(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2.(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>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.</p> <p> <b>NOTE:</b> The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.</p>						
<b>Example</b>	<pre>Dell#show ip rpf RPF information for 10.10.10.9   RPF interface: Te 0/4   RPF neighbor: 165.87.31.4   RPF route/mask: 10.10.10.9/255.255.255.255   RPF type: unicast</pre>						

## IPv6 Multicast Commands

The following section contains the IPv6 multicast commands.

### debug ipv6 mld\_host

Enable the collection of debug information for MLD host transactions.

<b>Syntax</b>	<pre>[no] debug ipv6 mld_host [<i>int-count</i>   <i>interface type</i>] [<i>slot/port-range</i>]</pre> <p>To discontinue collection of debug information for the MLD host transactions, use the <code>no debug ipv6 mld_host</code> command.</p>						
<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b><i>int-count</i></b></td> <td>Enter the keyword <code>count</code> to indicate the number of required debug messages.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>interface type</i></b></td> <td>           Enter the following keywords and slot/port information:           <ul style="list-style-type: none"> <li>• For a 10G Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information.</li> <li>• For a management interface, enter the keyword <code>managementinterface</code> then the slot/port information.</li> <li>• For a port-channel interface, enter the keywords <code>port-channel</code> then the slot/port information.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then the slot/port information.</li> </ul> </td> </tr> </table>	<b><i>int-count</i></b>	Enter the keyword <code>count</code> to indicate the number of required debug messages.	<b><i>interface type</i></b>	Enter the following keywords and slot/port information: <ul style="list-style-type: none"> <li>• For a 10G Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information.</li> <li>• For a management interface, enter the keyword <code>managementinterface</code> then the slot/port information.</li> <li>• For a port-channel interface, enter the keywords <code>port-channel</code> then the slot/port information.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then the slot/port information.</li> </ul>		
<b><i>int-count</i></b>	Enter the keyword <code>count</code> to indicate the number of required debug messages.						
<b><i>interface type</i></b>	Enter the following keywords and slot/port information: <ul style="list-style-type: none"> <li>• For a 10G Ethernet interface, enter the keyword <code>tengigabitethernet</code> then the slot/port information.</li> <li>• For a management interface, enter the keyword <code>managementinterface</code> then the slot/port information.</li> <li>• For a port-channel interface, enter the keywords <code>port-channel</code> then the slot/port information.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then the slot/port information.</li> </ul>						
<b>Default</b>	Disabled						
<b>Command Modes</b>	EXEC						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2.(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2.(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2.(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>To debug the MLD protocol for all ports or for specified ports, use the <code>debug ipv6 mld_host</code> command. Displayed information includes when a query is received, when a report is sent, when a mcast joins or leaves a group, and some reasons why an MLD query is rejected.</p>						

# ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

**Syntax** `ip multicast-limit limit`

**Parameters** *limit* Enter the desired maximum number of multicast entries on the system. The range is from 1 to 50000.

**Defaults** **15000** routes.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

# Neighbor Discovery Protocol (NDP)

The Dell Networking Operating System (OS) supports the network discovery protocol for IPv6.

The neighbor discovery protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP uses the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

## Topics:

- [clear ipv6 neighbors](#)
- [ipv6 neighbor](#)
- [show ipv6 neighbors](#)


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

**Command Modes**

- EXEC
- EXEC Privilege


**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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		
<b>ipv6-address</b>	Enter the IPv6 address of the neighbor in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zero.
<b>interface interface</b>	Enter the keyword <code>interface</code> then the interface type and slot/port or number information:	<ul style="list-style-type: none"><li>• For a Fast Ethernet interface, enter the keyword <code>fastEthernet</code> then the slot/port information.</li><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number.</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul>
<b>hardware_addresses</b>	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.	

**Defaults** none

**Command Modes** CONFIGURATION



**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all the IPv6 neighbor addresses stored on the control processor (CP).

**Syntax** `show ipv6 neighbors [vrf vrf-name] [ipv6-address| interface interface]`

Parameters		
<b>vrf vrf-name</b>	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to display the neighbors corresponding to that VRF.	 <b>NOTE:</b> If you do not specify this option, neighbors corresponding to the default VRF are displayed.
<b>ipv6-address</b>	Enter the IPv6 address of the neighbor in the x:x:x:x format.	 <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zero.



**interface**  
**interface**

Enter the keyword `interface` then the interface type and slot/port or number information:

- For a Fast Ethernet interface, enter the keyword `fastEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell# show ipv6 neighbors
IPv6 Address Expires(min) Hardware Address State Interface VLAN CPU
-----
100::1 0.03 00:00:00:00:00:22 DELAY Te 1/12 - CP
fe80::200:ff:fe00:22 232 00:00:00:00:00:22 STALE Te 1/12 - CP
500::1 0.60 00:01:e8:17:5c:af REACH Te 1/13 - CP
fe80::200:ff:fe00:17 232 00:00:00:00:00:29 REACH Te 1/14 - CP
900::1 0.60 00:01:e8:17:5c:b1 STALE Po 23 - CP
400::1 0.60 00:01:e8:17:5c:ae REACH Te 1/2 V1 100 CP
Dell#
```

# NPIV Proxy Gateway

The N-port identifier virtualization (NPIV) Proxy Gateway (NPG) feature provides FCoE-FC bridging capability on the FN IOM with the FC Flex IO module switch, allowing server CNAs to communicate with SAN fabrics over the FN IOM with the FC Flex IO module.

To configure the FN I/OM with the FC Flex IO module to operate as an NPIV proxy gateway, use the following commands:

## Topics:

- [dcb-map](#)
- [description \(for FCoE maps\)](#)
- [fabric-id vlan](#)
- [fcf-priority](#)
- [fc-map](#)
- [fcoe-map](#)
- [feature fc](#)
- [fka-adv-period](#)
- [keepalive](#)
- [show fcoe-map](#)
- [show fc sw](#)
- [show interfaces status](#)
- [show npiv devices](#)
- [show qos dcb-map](#)
- [show running-config fcoe-map](#)

## 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** `map-name` Enter a DCB map name. The maximum number of alphanumeric characters is 32.

**Defaults** None.

**Command Modes** CONFIGURATION  
INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS).

To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command.

Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default.

The `dcb-map` command is supported only on physical Ethernet interfaces.

To remove a DCB map from an interface, enter the `no dcb-map map-name` command in Interface configuration mode.

#### Related Commands

[show qos dcb-map](#)— displays the dcb-map profiles configured on the system.

[dcb-map stack-unit all stack-ports all](#)— applies a DCB map on all ports of a switch stack.

## description (for FCoE maps)

In an FCoE map, add a text description of the FCoE and FC parameters used to transmit storage traffic over an FN 2210S Aggregator and M I/O Aggregator NPIV proxy gateway in a converged fabric.

**Syntax** `description text`

**Parameters** `text` Enter a maximum of 32 characters.

**Defaults** None

**Command Modes** FCOE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Supported on the FN 2210S Aggregator.
9.3(0.0)	Supported on the M I/O Aggregator.

#### Usage Information

The text description is displayed in `show fcoe-map` command output.

#### Related Commands

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#)— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fabric-id vlan

In an FCoE map, configure the association between the dedicated VLAN used to carry FCoE traffic between servers and a SAN, and the fabric where the desired storage arrays are installed.

**Syntax** `fabric-id fabric-num vlan vlan-id`

**Parameters**

<code>fabric-id fabric-num</code>	Enter a fabric ID number that is the same as the ID number of the dedicated VLAN used to carry FCoE storage traffic to the fabric specified in the FCoE map. You can enter a fabric ID in the range 2–4094.
<code>vlan vlan-id</code>	Enter the ID number of the dedicated VLAN used to carry FCoE storage traffic between servers and a SAN fabric and specified with the <code>vlan</code> command in the FCoE map.

**Defaults** None

**Command Modes** FCOE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information**

In the `fabric-id vlan` command, the fabric and VLAN ID numbers must be the same.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique.

To remove a fabric-VLAN association from an FCoE map, enter the `no fabric-id vlan` command.

Create a VLAN and then specify the configured VLAN ID in the `fabric-id vlan` command. Otherwise, the following error message is displayed.

```
Dell(conf-fcoe-f)#fabric-id 10 vlan 10 % Error: Vlan 10 does not exist
```

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fcf-priority

In an FCoE map, configure the priority used by a server CNA to select an upstream FCoE forwarder (FCF).

**Syntax** `fcf-priority priority`

**Parameters**

***priority*** Enter the priority assigned to the FN 2210S Aggregator NPIV proxy gateway, which appears to a downstream server CNA as an FCF. The range of FCF priority values is from 1 to 255.

**Defaults** 128

**Command Modes** FCOE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

The FCF priority you assign to an FN 2210S Aggregator is used by server CNAs to select an upstream FCF to use for a fabric login (FLOGI).

To remove a configured FCF priority from an FCoE map, enter the `no fcf-priority` command.

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

# fc-map

In an FCoE map, configure the FCoE mapped address prefix (FC-MAP) value which is used to identify FCoE traffic transmitted on the FCoE VLAN for the specified fabric.

**Syntax** `fc-map fc-map-value`

**Parameters** **fc-map-value** Enter the unique MAC address prefix used by a SAN fabric.  
The range of FC-MAP values is from 0EFC00 to 0EFCFF.

**Defaults** None

**Command Modes** FCoE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

The FC-MAP value you enter must match the FC-MAP value used by an FC switch or FCoE forwarder (FCF) in the fabric. An FCF switch accepts only FCoE traffic that uses the correct FC-MAP value.

The FC-MAP value is used to generate the fabric-provided MAC address (FP-MAC). The FPMA is used by servers to transmit FCoE traffic to the fabric. An FC-MAP can be associated with only one FCoE VLAN and vice versa.

In an FCoE map, the FC-MAP value, fabric ID, and FCoE VLAN parameters must be unique.

To remove a configured FC-MAP value from an FCoE map, enter the `no fc-map` command.

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

# fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

**Syntax** `fcoe-map map-name`

**Parameters** **map-name** Maximum: 32 alphanumeric characters.

**Defaults** On the FN2210S Aggregator with PMUX modules, the following parameters are applied on all the PMUX module interfaces:

- Description: SAN\_FABRIC
- Fabric-id: 1002
- Fcoe-vlan: 1002
- Fc-map: 0x0efc00
- Fcf-priority: 128
- Fka-adv-period: 8000mSec

- Keepalive: enable
- Vlan priority: 3

**Command Modes** CONFIGURATION  
INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Supported on the FN2210S Aggregator with the PMUX module.
9.3(0.0)	Introduced on the M I/O Aggregator with the PMUX module.

**Usage Information**

An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on an FN2210S Aggregator with the PMUX module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric.

On an FN2210S Aggregator a with the PMUX module NPIV proxy gateway, you cannot apply an FCoE map applied on fabric-facing FC ports and server-facing 10-Gigabit Ethernet ports.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN used for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority used by a server, and the FIP keepalive (FKA) advertisement timeout.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique. Use one FCoE map to access one SAN fabric. You cannot use the same FCoE map to access different fabrics.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map map-name` command in Interface configuration mode.

**Related Commands**

[show fcoe-map](#)— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## feature fc

Enables the Fibre channel communication via the NPG functionality.

**Syntax** `feature fc`

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Default** Enabled

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Supported on the FN I/O Aggregator.
9.3(0.0)	Supported on the M I/O Aggregator.

**Usage Information** The command is supported only in FN2210S Aggregator.

## fka-adv-period

In an FCoE map, configure the time interval used to transmit FIP keepalive (FKA) advertisements.

**Syntax** `fka-adv-period seconds`

**Parameters** **seconds** Enter the time period (in seconds) used to send FIP keepalive messages to peer devices. The range is from 8 to 90 seconds.

**Defaults** 8 seconds

**Command Modes** FCoE MAP

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information** To delete the FIP keepalive time period from an FCoE map, enter the `no fka-adv-erpiod` command.

**Related Commands** [fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## keepalive

In an FCoE map, enable the monitoring of FIP keepalive messages (if it is disabled).

**Syntax** `keepalive`

**Parameters** None

**Defaults** FIP keepalive monitoring is enabled on Ethernet and Fibre Channel interfaces.

**Command Modes** FCoE MAP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information** FIP keepalive (FKA) messaging is used to detect if other FCoE devices are reachable.

To remove FIP keepalive monitoring from an FCoE map, enter the `no keepalive` command.

**Related Commands** [fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

# show fcoe-map

Displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

**Syntax** `show fcoe-map [brief | map-name]`

**Parameters**

- brief** Displays an overview of currently configured FCoE maps.
- map-name** Displays the FC and FCoE configuration parameters in a specified FCoE map. The FCoE map is applied on Ethernet (FCoE) and FC ports to transmit FC storage traffic to a specified fabric.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.6(0.0)	Supported on the FN2210S Aggregator.
	9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information** Use the `show fcoe-map` command to display the FC and FCoE parameters used to configure server-facing Ethernet (FCoE) and fabric-facing FC ports in all FCoE maps on an FN 2210S Aggregator with the FC Flex IO module NPIV proxy gateway.

In each FCoE map, the values for the fabric ID and FC-MAP that identify the SAN fabric to which FC storage traffic is sent, and the FCoE VLAN to be used must be unique.

The following describes the `show fcoe-map brief` output shown in the example.

Field	Description
<b>Fabric-Name</b>	Name of a SAN fabric.
<b>Fabric ID</b>	The ID number of the SAN fabric to which FC traffic is forwarded.
<b>VLAN ID</b>	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
<b>FC-MAP</b>	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
<b>FCF Priority</b>	The priority used by a server to select an upstream FCoE forwarder.
<b>Config-State</b>	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
<b>Oper-State</b>	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).

The following describes the `show fcoe-map map-name` output shown in the example.

Field	Description
<b>Fabric-Name</b>	Name of a SAN fabric.
<b>Fabric ID</b>	The ID number of the SAN fabric to which FC traffic is forwarded.



Field	Description
<b>VLAN ID</b>	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
<b>VLAN priority</b>	FCoE traffic uses VLAN priority 3. (This setting is not user-configurable.)
<b>FC-MAP</b>	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
<b>FKA-ADV-period</b>	Time interval (in seconds) used to transmit FIP keepalive advertisements.
<b>FCF Priority</b>	The priority used by a server to select an upstream FCoE forwarder.
<b>Config-State</b>	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
<b>Oper-State</b>	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).
<b>Members</b>	FN2210S Aggregator with the FC Flex IO module Ethernet and FC ports that are members of the dedicated FCoE VLAN that carries storage traffic to the specified fabric.

### Example

```
Dell#show fcoe-map brief
Fabric-Name Fabric-Id Vlan-Id FC-MAP FCF-Priority Config-State Oper-State
test        16          16      0efc02  128      ACTIVE     UP
cnatest     1003        1003    0efc03  128      ACTIVE     UP
sitest      1004        1004    0efc04  128      ACTIVE     DOWN
```

```
Dell#show fcoe-map si

Fabric Name      si
Fabric Id       1004
Vlan Id         1004
Vlan priority    3
FC-MAP          0efc04
FKA-ADV-Period  8
Fcf Priority     128
Config-State    ACTIVE
Oper-State      DOWN
Members
```

### Related Commands

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

## show fc sw

Display the switch configuration for Fibre Channel capability.

**Syntax** `show fc sw`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All modes

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.6(0.0)	Supported on the FN2210S Aggregator.
9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

### Example

```
Dell(conf)#do show fc sw
Switch Mode : NPG
Switch WWN   : 10:00:00:1e:c9:f1:00:d7
```

## show interfaces status

Displays a summary of interface information or specify a stack unit and interface to display status information for that specific interface only.

**Syntax** `show interfaces [interface | stack-unit unit-number] status`

**Parameters**

- interface*** (OPTIONAL) Enter one of the following keywords and slot/port or number information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- linecard slot-number*** (OPTIONAL) Enter the keyword `linecard` then the slot number.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.6(0.0)	Supported on the FN 2210S Aggregator.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	9.3(0.0)	Supported on the M I/O Aggregator.

### Example

```
Dell#show interface status
Port      Description  Status  Speed    Duplex  Vlan
Te 0/1    Te 0/1       Up      10000   Mbit Full 1-4094
Te 0/2    Te 0/2       Up      10000   Mbit Full 1-4094
Te 0/3    Te 0/3       Up      10000   Mbit Full 1-4094
Te 0/4    Te 0/4       Up      10000   Mbit Full 1-4094
Te 0/5    Te 0/5       Up      10000   Mbit Full --
Te 0/6    Te 0/6       Up      10000   Mbit Full 1-4094
Te 0/7    Te 0/7       Up      10000   Mbit Full --
Te 0/8    Te 0/8       Up      10000   Mbit Full --
Te 0/9    Te 0/9       Up      10000   Mbit Full --
Te 0/10   Te 0/10      Up      10000   Mbit Full --
Te 0/11   Te 0/11      Up      10000   Mbit Full --
Te 0/12   Te 0/12      Up      10000   Mbit Full --
Dell#
```

# show npiv devices

Displays the FCoE and FC devices currently logged into an FN I/O Aggregator Switch with the FC Flex IO module NPIV proxy gateway.

**Syntax** `show npiv devices [brief]`

**Parameters** **brief** Displays an overview of current server CNA-fabric connections over an FN I/O Aggregator with the FC Flex IO module NPIV proxy gateway.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** All modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.6.(0.0)	Supported on the FN2210S Aggregator.
	9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information** Use the `show npiv devices` command to display information on the server CNA, server-facing Ethernet and fabric-facing FC ports, and the SAN fabric in each server-fabric connection over an FN I/O Aggregator with the FC Flex IO module NPIV proxy gateway.

The following describes the `show npiv devices brief` output shown in the example.

Field	Description
<b>ENode-Intf</b>	FN I/O Aggregator with the FC Flex IO module Ethernet interface ( <i>slot/port</i> ) to which a server CNA is connected.
<b>ENode-WWPN</b>	Worldwide port name (WWPN) of a server CNA port.
<b>FCoE-Vlan</b>	VLAN ID of the dedicated VLAN used to transmit FCoE traffic to and from the fabric.
<b>Fabric-Intf</b>	Fabric-facing Fibre Channel port ( <i>slot/port</i> ) on which FC traffic is transmitted to the specified fabric.
<b>Fabric-Map</b>	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
<b>LoginMethod</b>	Method used by the server CNA to log in to the fabric; for example: FLOGI - ENode logged in using a fabric login (FLOGI). FDISC - ENode logged in using a fabric discovery (FDISC).
<b>Status</b>	Operational status of the link between a server CNA port and a SAN fabric: Logged In - Server has logged in to the fabric and is able to transmit FCoE traffic.

## Example

```
Dell# show npiv devices brief
Total NPIV Devices = 2
-----
ENode-Intf ENode-WWPN FCoE-Vlan abric-Intf Fabric-Map LginMethod Status
-----
Te 0/12 20:01:00:10:18:f1:94:20 1003 Fc 0/5 fid_1003 FLOG LOGGED_IN
Te 0/13 10:00:00:00:c9:d9:9c:cb 1003 Fc 0/0 fid_1003 FDISC LOGGED_IN
```

**Usage Information** The following describes the `show npiv devices` output shown in the example.

Field	Description
<b>ENode</b> [ <i>number</i> ]	A server CNA that has successfully logged in to a fabric over an FN I/O Aggregator with the FC Flex IO module Ethernet port in ENode mode.
<b>ENode MAC</b>	MAC address of a server CNA port.
<b>ENode Intf</b>	Port number of a server-facing Ethernet port operating in ENode mode.
<b>FCF MAC</b>	Fibre Channel forwarder MAC: MAC address of FN I/O Aggregator Switch with the FC Flex IO module FCF interface.
<b>Fabric Intf</b>	Fabric-facing Fibre Channel port ( <i>slot/port</i> ) on which FCoE traffic is transmitted to the specified fabric.
<b>FCoE VLAN</b>	ID of the dedicated VLAN used to transmit FCoE traffic from a server CNA to a fabric and configured on both the server-facing FN I/O Aggregator with the FC Flex IO module port and server CNA port.
<b>Fabric Map</b>	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
<b>ENode WWPN</b>	Worldwide port name of the server CNA port.
<b>ENode WWNN</b>	Worldwide node name of the server CNA.
<b>FCoE MAC</b>	Fabric-provided MAC address (FPMA). The FPMA consists of the FC-MAP value in the FCoE map and the FC-ID provided by the fabric after a successful FLOGI. In the FPMA, the most significant bytes are the FC-MAP; the least significant bytes are the FC-ID.
<b>FC-ID</b>	FC port ID provided by the fabric.
<b>LoginMethod</b>	Method used by the server CNA to log in to the fabric; for example, FLOGI or FDISC.
<b>Secs</b>	Number of seconds that the fabric connection is up.
<b>State</b>	Status of the fabric connection: logged in.

### Example

```

ENode[0]:
ENode MAC      : 00:10:18:f1:94:21
ENode Intf     : Te 0/12
FCF MAC       : 5c:f9:dd:ef:10:c8
Fabric Intf    : Fc 0/5
FCoE Vlan     : 1003
Fabric Map     : fid_1003
ENode WWPN    : 20:01:00:10:18:f1:94:20
ENode WWNN    : 20:00:00:10:18:f1:94:21
FCoE MAC      : 0e:fc:03:01:02:01
FC-ID         : 01:02:01
LoginMethod    : FLOGI
Secs          : 5593
Status        : LOGGED_IN

ENode[1]:
ENode MAC      : 00:10:18:f1:94:22
ENode Intf     : Te 0/13
FCF MAC       : 5c:f9:dd:ef:10:c9
Fabric Intf    : Fc 0/0
FCoE Vlan     : 1003
Fabric Map     : fid_1003
ENode WWPN    : 10:00:00:00:c9:d9:9c:cb
ENode WWNN    : 10:00:00:00:c9:d9:9c:cd
FCoE MAC      : 0e:fc:03:01:02:02
FC-ID         : 01:02:01
LoginMethod    : FDISC
Secs          : 5593
Status        : LOGGED_IN

```

### Related Commands

[dcb-map](#)— creates a DCB map to configure DCB parameters on Ethernet ports that support converged Ethernet traffic.

`fcoe-map` — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

## show qos dcb-map

Display the DCB parameters configured in a specified DCB map.

**Syntax** `show qos dcb-map map-name`

**Parameters** `map-name` Displays the PFC and ETS parameters configured in the specified map.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Supported on the FN I/O Aggregator.
9.6(0.0)	Supported on the M I/O Aggregator.

### Usage Information

Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
<b>State</b>	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
<b>PFC Mode</b>	PFC configuration in DCB map: On (enabled) or Off.
<b>PG</b>	Priority group configured in the DCB map.
<b>TSA</b>	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
<b>BW</b>	Percentage of bandwidth allocated to the priority group.
<b>PFC</b>	PFC setting for the priority group: On (enabled) or Off.
<b>Priorities</b>	802.1p priorities configured in the priority group.

### Example

```
Dell# show qos dcb-map dcbmap2

State      :Complete
PfcMode:ON
-----
PG:0 TSA:ETS BW:50 PFC:OFF
Priorities:0 1 2 4 5 6 7

PG:1 TSA:ETS BW:50 PFC:ON
Priorities:3
```

# show running-config fcoe-map

Displays the current fcoe-map configurations.

**Syntax** show running-config fcoe-map

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

## Example

```
Dell(conf)#do show running-config fcoe-map
!
fcoe-map map
fc-map 0efc00
fabric-id 100 vlan 100
```

# Open Shortest Path First (OSPFv2 and OSPFv3)

The Switch supports open shortest path first version 2 (OSPFv2) for IPv4 and version 3 (OSPFv3) for IPv6. Up to 16 OSPF instances can be run simultaneously on the Switch.

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.

- [OSPFv2 Commands](#)
- [OSPFv3 Commands](#)

## Topics:

- [OSPFv2 Commands](#)
- [area default-cost](#)
- [area nssa](#)
- [area range](#)
- [area stub](#)
- [auto-cost](#)
- [clear ip ospf](#)
- [clear ip ospf statistics](#)
- [debug ip ospf](#)
- [default-information originate](#)
- [default-metric](#)
- [description](#)
- [distance](#)
- [distance ospf](#)
- [distribute-list in](#)
- [distribute-list out](#)
- [fast-convergence](#)
- [flood-2328](#)
- [graceful-restart grace-period](#)
- [graceful-restart helper-reject](#)
- [graceful-restart mode](#)
- [graceful-restart role](#)
- [ip ospf auth-change-wait-time](#)
- [ip ospf authentication-key](#)
- [ip ospf cost](#)
- [ip ospf dead-interval](#)
- [ip ospf hello-interval](#)
- [ip ospf message-digest-key](#)
- [ip ospf mtu-ignore](#)
- [ip ospf network](#)
- [ip ospf priority](#)
- [ip ospf retransmit-interval](#)
- [ip ospf transmit-delay](#)

- log-adjacency-changes
- maximum-paths
- mib-binding
- network area
- passive-interface
- redistribute
- redistribute bgp
- redistribute isis
- router-id
- router ospf
- show config
- show ip ospf
- show ip ospf asbr
- show ip ospf database
- show ip ospf database asbr-summary
- show ip ospf database external
- show ip ospf database network
- show ip ospf database nssa-external
- show ip ospf database opaque-area
- show ip ospf database opaque-as
- show ip ospf database opaque-link
- show ip ospf database router
- show ip ospf database summary
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf routes
- show ip ospf statistics
- show ip ospf timers rate-limit
- show ip ospf topology
- summary-address
- timers spf
- timers throttle lsa all
- timers throttle lsa arrival
- OSPFv3 Commands
- area authentication
- area encryption
- area nssa
- auto-cost
- clear ipv6 ospf process
- debug ipv6 ospf
- debug ipv6 ospf bfd
- debug ipv6 ospf events
- debug ipv6 ospf packet
- debug ipv6 ospf spf
- default-information originate
- graceful-restart grace-period
- graceful-restart mode
- ipv6 ospf area
- ipv6 ospf authentication
- ipv6 ospf bfd all-neighbors
- ipv6 ospf cost
- ipv6 ospf dead-interval
- ipv6 ospf encryption
- ipv6 ospf graceful-restart helper-reject
- ipv6 ospf hello-interval
- ipv6 ospf priority



- [ipv6 router ospf](#)
- [maximum-paths](#)
- [passive-interface](#)
- [redistribute](#)
- [router-id](#)
- [show crypto ipsec policy](#)
- [show crypto ipsec sa ipv6](#)
- [show ipv6 ospf database](#)
- [show ipv6 ospf interface](#)
- [show ipv6 ospf neighbor](#)
- [snmp context](#)
- [timers spf](#)

## 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.

**Syntax** `area area-id default-cost cost`

To return default values, use the `no area area-id default-cost` command.

**Parameters**

<b><i>area-id</i></b>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
<b><i>cost</i></b>	Specifies the stub area's advertised external route metric. The range is from zero (0) to 65535.

**Defaults** `cost = 1`; no areas are configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** In the Dell Networking operating software, `cost` is defined as reference bandwidth.

**Related Commands** [area stub](#) — creates a stub area.

### area nssa

Specify an area as a not so stubby area (NSSA).

**Syntax** `area area-id nssa [default-information-originate] [no-redistribution] [no-summary]`

To delete an NSSA, use the `no area area-id nssa` command.

<b>Parameters</b>	<b><i>area-id</i></b>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	<b>no-redistribution</b>	(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).
	<b>default-information-originate</b>	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
	<b>no-summary</b>	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER OSPF	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## area range

Summarize routes matching an address/mask at an area border router (ABR).

<b>Syntax</b>	<code>area area-id range ip-address mask [not-advertise]</code>	
	To disable route summarization, use the <code>no area area-id range ip-address mask</code> command.	
<b>Parameters</b>	<b><i>area-id</i></b>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
	<b><i>ip-address</i></b>	Specify an IP address in dotted decimal format.
	<b><i>mask</i></b>	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
	<b>not-advertise</b>	(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.)
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER OSPF	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.	
<b>Related Commands</b>	<a href="#">area stub</a> — creates a stub area.	
	<a href="#">router ospf</a> — enters ROUTER OSPF mode to configure an OSPF instance.	

# area stub

Configure a stub area, which is an area not connected to other areas.

<b>Syntax</b>	<code>area area-id stub [no-summary]</code> To delete a stub area, use the <code>no area area-id stub</code> command.						
<b>Parameters</b>	<table><tr><td><b>area-id</b></td><td>Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.</td></tr><tr><td><b>no-summary</b></td><td>(OPTIONAL) Enter the keywords <code>no-summary</code> to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.</td></tr></table>	<b>area-id</b>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.	<b>no-summary</b>	(OPTIONAL) Enter the keywords <code>no-summary</code> to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.		
<b>area-id</b>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.						
<b>no-summary</b>	(OPTIONAL) Enter the keywords <code>no-summary</code> to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.						
<b>Defaults</b>	Disabled.						
<b>Command Modes</b>	ROUTER OSPF						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	To configure all routers and access servers within a stub, use this command.						
<b>Related Commands</b>	<code>router ospf</code> — 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.

<b>Syntax</b>	<code>auto-cost [reference-bandwidth ref-bw]</code> To return to the default bandwidth or to assign cost based on the interface type, use the <code>no auto-cost [reference-bandwidth]</code> command.						
<b>Parameters</b>	<table><tr><td><b>ref-bw</b></td><td>(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is <b>100 megabits per second</b>.</td></tr></table>	<b>ref-bw</b>	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is <b>100 megabits per second</b> .				
<b>ref-bw</b>	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is <b>100 megabits per second</b> .						
<b>Defaults</b>	<b>100 megabits per second.</b>						
<b>Command Modes</b>	ROUTER OSPF						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

# clear ip ospf

Clear all OSPF routing tables.

<b>Syntax</b>	<code>clear ip ospf process-id [process]</code>
---------------	---

<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
	<b><i>process</i></b>	(OPTIONAL) Enter the keyword <code>process</code> to reset the OSPF process.
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

<b>Syntax</b>	<code>clear ip ospf process-id statistics [interface name {neighbor router-id}]</code>	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
	<b><i>interface name</i></b>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
	<b><i>neighbor router-id</i></b>	(OPTIONAL) Enter the keyword <code>neighbor</code> then the neighbor's router-id in dotted decimal format (A.B.C.D.).
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">show ip ospf statistics</a> — 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.

<b>Syntax</b>	<code>debug ip ospf process-id [bfd   event   packet   spf   database-timer rate-limit]</code>	
	To cancel the debug command, use the <code>no debug ip ospf</code> command.	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.

<b>bfd</b>	(OPTIONAL) Enter the keyword <code>bfd</code> to debug only OSPF BFD information.
<b>event</b>	(OPTIONAL) Enter the keyword <code>event</code> to debug only OSPF event information.
<b>packet</b>	(OPTIONAL) Enter the keyword <code>packet</code> to debug only OSPF packet information.
<b>spf</b>	(OPTIONAL) Enter the keyword <code>spf</code> to display the Shortest Path First information.
<b>database-timer rate-limit</b>	(OPTIONAL) Enter the keywords <code>database-timer rate-limit</code> to display the LSA throttling timer information.

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `debug ip ospf` command shown in the Example below.

Field	Description
<b>8:14</b>	Displays the time stamp.
<b>OSPF</b>	Displays the OSPF process ID: instance ID.
<b>v:</b>	Displays the OSPF version. The system supports version 2 only.
<b>t:</b>	Displays the type of packet sent: <ul style="list-style-type: none"> <li>• 1 - Hello packet</li> <li>• 2 - database description</li> <li>• 3 - link state request</li> <li>• 4 - link state update</li> <li>• 5 - link state acknowledgement</li> </ul>
<b>l:</b>	Displays the packet length.
<b>rid:</b>	Displays the OSPF router ID.
<b>aid:</b>	Displays the Autonomous System ID.
<b>chk:</b>	Displays the OSPF checksum.
<b>aut:</b>	States if OSPF authentication is configured. One of the following is listed: <ul style="list-style-type: none"> <li>• 0 - no authentication configured</li> <li>• 1 - simple authentication configured using the <code>ip ospf authentication-key</code> command</li> <li>• 2 - MD5 authentication configured using the <code>ip ospf message-digest-key</code> command</li> </ul>
<b>auk:</b>	If the <code>ip ospf authentication-key</code> command is configured, this field displays the key used.
<b>keyid:</b>	If the <code>ip ospf message-digest-key</code> command is configured, this field displays the MD5 key
<b>to:</b>	Displays the interface to which the packet is intended.
<b>dst:</b>	Displays the destination IP address.
<b>netmask:</b>	Displays the destination IP address mask.
<b>pri:</b>	Displays the OSPF priority
<b>N, MC, E, T</b>	Displays information available in the Options field of the HELLO packet: <ul style="list-style-type: none"> <li>• N + (N-bit is set)</li> <li>• N - (N-bit is not set)</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets)</li> <li>MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets)</li> <li>E + (router is able to accept AS External LSAs)</li> <li>E - (router cannot accept AS External LSAs)</li> <li>T + (router can support TOS)</li> <li>T - (router cannot support TOS)</li> </ul>
<b>hi:</b>	Displays the amount of time configured for the HELLO interval.
<b>di:</b>	Displays the amount of time configured for the DEAD interval.
<b>dr:</b>	Displays the IP address of the designated router.
<b>bdr:</b>	Displays the IP address of the Border Area Router.

### Example

```
Dell#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

Dell#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
      aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Gi 4/3 dst:224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

## default-information originate

To generate a default external route into an OSPF routing domain, configure the system.

**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		
<b>always</b>	(OPTIONAL) Enter the keyword <code>always</code> to specify that default route information must always be advertised.	
<b>metric <i>metric-value</i></b>	(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.	
<b>metric-type <i>type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then an OSPF link state type of 1 or 2 for default routes. The values are: <ul style="list-style-type: none"> <li>1 = Type 1 external route</li> <li>2 = Type 2 external route</li> </ul>	
<b>route-map <i>map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of an established route map.	

**Defaults** Disabled.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes**       Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**      [redistribute](#) — redistributes routes from other routing protocols into OSPF.

## description

Add a description about the selected OSPF configuration.

**Syntax**                    `description description`  
To remove the OSPF description, use the `no description` command.

**Parameters**              *description*              Enter a text string description to identify the OSPF configuration (80 characters maximum).

**Defaults**                 none

**Command Modes**         ROUTER OSPF

**Supported Modes**       Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**      [show ip ospf asbr](#) — displays the VLAN configuration.

## distance

Define an administrative distance for particular routes to a specific IP address.

**Syntax**                    `distance weight [ip-address mask access-list-name]`  
To delete the settings, use the `no distance weight [ip-address mask access-list-name]` command.

<b>Parameters</b>	<b><i>weight</i></b>	Specify an administrative distance. The range is from 1 to 255. The default is <b>110</b> .
	<b><i>ip-address</i></b>	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, include the mask for that router address.
	<b><i>mask</i></b>	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
	<b><i>access-list-name</i></b>	(OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.

**Defaults** 110

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## distance ospf

Configure an OSPF distance metric for different types of routes.

**Syntax** `distance ospf [external dist3] [inter-area dist2] [intra-area dist1]`  
 To delete these settings, use the `no distance ospf` command.

<b>Parameters</b>	<b><i>external dist3</i></b>	(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 <b>110</b> .
	<b><i>inter-area dist2</i></b>	(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 <b>110</b> .
	<b><i>intra-area dist1</i></b>	(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 <b>110</b> .

- Defaults**
- `external dist3` = **110**
  - `inter-area dist2` = **110**
  - `intra-area dist1` = **110**

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To specify a distance for routes learned from other routing domains, use the `redistribute` command.

## distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

**Syntax** `distribute-list prefix-list-name in [interface]`  
 To delete a filter, use the `no distribute-list prefix-list-name in [interface]` command.



<b>Parameters</b>	<b><i>prefix-list-name</i></b>	Enter the name of a configured prefix list.
	<b><i>interface</i></b>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

**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.

<b>Parameters</b>	<b><i>prefix-list-name</i></b>	Enter the name of a configured prefix list.
	<b>bgp</b>	(OPTIONAL) Enter the keyword <code>bgp</code> to specify that BGP routes are distributed.
	<b>connected</b>	(OPTIONAL) Enter the keyword <code>connected</code> to specify that connected routes are distributed.
	<b>isis</b>	(OPTIONAL) Enter the keyword <code>isis</code> to specify that IS-IS routes are distributed.
	<b>rip</b>	(OPTIONAL) Enter the keyword <code>rip</code> to specify that RIP routes are distributed.
	<b>static</b>	(OPTIONAL) Enter the keyword <code>static</code> to specify that only manually configured routes are distributed.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description heading</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `fast-convergence {number}`

To cancel fast-convergence, use the `no fast convergence` command.

**Parameters** *number* Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is from 1 to 4.


**Defaults** none.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `flood-2328`

To disable, use the `no flood-2328` command.

**Defaults** Disabled.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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, the system 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 the system 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.

<b>Syntax</b>	<code>graceful-restart grace-period <i>seconds</i></code> To disable the grace period, use the <code>no graceful-restart grace-period</code> command.						
<b>Parameters</b>	<b><i>seconds</i></b> 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.						
<b>Defaults</b>	Not Configured						
<b>Command Modes</b>	ROUTER OSPF						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

## graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

<b>Syntax</b>	<code>graceful-restart helper-reject <i>ip-address</i></code> To return to default value, use the <code>no graceful-restart helper-reject</code> command.						
<b>Parameters</b>	<b><i>ip-address</i></b> Enter the OSPF router-id, in IP address format, of the restart router that <i>will not</i> act as a helper during graceful restart.						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	ROUTER OSPF						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

## graceful-restart mode

Enable the graceful restart mode.

<b>Syntax</b>	<code>graceful-restart mode [planned-only   unplanned-only]</code> To disable graceful restart mode, use the <code>no graceful-restart mode</code> command.
<b>Parameters</b>	<b>planned-only</b> (OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only. <b>unplanned-only</b> (OPTIONAL) Enter the keywords <code>unplanned-only</code> to indicate graceful restart is supported in an unplanned restart condition only.
<b>Defaults</b>	Support for both planned and unplanned failures.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## graceful-restart role

Specify the role for your OSPF router during graceful restart.

**Syntax** `graceful-restart role [helper-only | restart-only]`  
To disable graceful restart role, use the `no graceful-restart role` command.

**Parameters**

<b>role helper-only</b>	(OPTIONAL) Enter the keywords <code>helper-only</code> to specify the OSPF router is a helper only during graceful restart.
<b>role restart-only</b>	(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

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

**Syntax** `ip ospf auth-change-wait-time seconds`  
To return to the default, use the `no ip ospf auth-change-wait-time` command.

**Parameters** **seconds** Enter the seconds. The range is from 0 to 300.

**Defaults** **zero (0) seconds.**

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

<b>Syntax</b>	<code>ip ospf authentication-key [encryption-type] key</code> To delete an authentication key, use the <code>no ip ospf authentication-key</code> command.						
<b>Parameters</b>	<b>encryption-type</b> (OPTIONAL) Enter 7 to encrypt the key. <b>key</b> Enter an eight-character string. Strings longer than eight characters are truncated.						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip ospf cost cost</code> To return to default value, use the <code>no ip ospf cost</code> command.						
<b>Parameters</b>	<b>cost</b> Enter a number as the cost. The range is from 1 to 65535.						
<b>Defaults</b>	The default cost is based on the reference bandwidth.						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.						
<b>Related Commands</b>	<a href="#">auto-cost</a> — 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.

<b>Syntax</b>	<code>ip ospf dead-interval seconds</code>
---------------	--

To return to the default values, use the `no ip ospf dead-interval` command.

<b>Parameters</b>	<b><i>seconds</i></b>	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is <b>40 seconds</b> .
<b>Defaults</b>	<b>40 seconds</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>		By default, the dead interval is four times the default hello-interval.
<b>Related Commands</b>	<a href="#">ip ospf hello-interval</a>	— sets the time interval between the hello packets.

## ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

<b>Syntax</b>	<code>ip ospf hello-interval seconds</code>	To return to the default value, use the <code>no ip ospf hello-interval</code> command.
<b>Parameters</b>	<b><i>seconds</i></b>	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is <b>10 seconds</b> .
<b>Defaults</b>	<b>10 seconds</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>		The time interval between the hello packets must be the same for routers in a network.
<b>Related Commands</b>	<a href="#">ip ospf dead-interval</a>	— 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.

<b>Syntax</b>	<code>ip ospf message-digest-key keyid md5key</code>	To delete a key, use the <code>no ip ospf message-digest-key keyid</code> command.
<b>Parameters</b>	<b><i>keyid</i></b>	Enter a number as the key ID. The range is from 1 to 255.
	<b><i>key</i></b>	Enter a continuous character string as the password.

**Defaults** No MD5 authentication is configured.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. The system sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell recommends keeping only one key per interface.

**NOTE:** The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

## ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

**Syntax** `ip ospf mtu-ignore`  
To return to the default, use the `no ip ospf mtu-ignore` command.

**Defaults** Enabled.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip ospf network

Set the network type for the interface.

**Syntax** `ip ospf network {broadcast | point-to-point}`  
To return to the default, use the `no ip ospf network` command.

**Parameters**

<b>broadcast</b>	Enter the keyword <code>broadcast</code> to designate the interface as part of a broadcast network.
<b>point-to-point</b>	Enter the keywords <code>point-to-point</code> to designate the interface as part of a point-to-point network.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

**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

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval must be larger for interfaces connected to virtual links.



## ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

**Syntax** `ip ospf transmit-delay seconds`  
To return to the default value, use the `no ip ospf transmit-delay` command.

**Parameters** ***seconds*** Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **1 second**.  
This value must be greater than the transmission and propagation delays for the interface.

**Defaults** **1 second**

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set the system.

**Syntax** `log-adjacency-changes`  
To disable the Syslog messages, use the `no log-adjacency-changes` command.

**Defaults** Disabled.

**Command Modes** ROUTER OSPF

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## maximum-paths

Enable the software to forward packets over multiple paths.

**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 16. 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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Added support for OSPFv3.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

**Syntax** `mib-binding`  
To mib-binding on this OSPF process, use the `no mib-binding` command.

**Defaults** none.

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `network ip-address mask area area-id`  
To disable an OSPF area, use the `no network ip-address mask area area-id` command.

**Parameters**

- ip-address*** Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
- mask*** Enter a network mask in /prefix format. (/x)
- area-id*** Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is from 0 to 65535. IP address format is dotted decimal format A.B.C.D.  
 **NOTE:** If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.


**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

## Syntax

```
passive-interface {default | interface}
```

To enable both the receiving and sending routing, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

## Parameters

### default

Enter the keyword `default` to make all OSPF interfaces (current and future) passive.

### interface

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

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

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

## Command History

### Version

### Description

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.19.1**

Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent using other interfaces.

The `default` keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the `no passive-interface interface` command. The `no` form of this command is inserted into the configuration for individual interfaces when the `no passive-interface interface` command is issued while `passive-interface default` is configured.

This command behavior has changed as follows:

```
passive-interface interface
```

- The previous `no passive-interface interface` is removed from the running configuration.
- The ABR status for the router is updated.
- Save `passive-interface interface` into the running configuration.

```
passive-interface default
```

- All present and future OSPF interfaces are marked as *passive*.
- Any adjacency is explicitly terminated from all OSPF interfaces.
- All previous `passive-interface interface` commands are removed from the running configuration.
- All previous `no passive-interface interface` commands are removed from the running configuration.

```
no passive-interface interface
```

- Remove the interface from the passive list.
- The ABR status for the router is updated.
- If `passive-interface default` is specified, then save `no passive-interface interface` into the running configuration.

No `passive-interface default`

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

## redistribute

Redistribute information from another routing protocol throughout the OSPF process.

**Syntax** `redistribute {connected | rip | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]`

To disable redistribution, use the `no redistribute {connected | isis | rip | static}` command.

<b>Parameters</b>	<b>connected</b>	Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.
	<b>rip</b>	Enter the keyword <code>rip</code> to specify that RIP routing information is redistributed.
	<b>static</b>	Enter the keyword <code>static</code> to specify that information from static routes is redistributed.
	<b>metric <i>metric-value</i></b>	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 16777214.
	<b>metric-type <i>type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: <ul style="list-style-type: none"> <li>• 1 = OSPF External type 1</li> <li>• 2 = OSPF External type 2</li> </ul>
	<b>route-map <i>map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
	<b>tag <i>tag-value</i></b>	(OPTIONAL) Enter the keyword <code>tag</code> then a number. The range is from 0 to 4294967295.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

**Related Commands** [default-information originate](#) — generates a default route into the OSPF routing domain.

# redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

**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] [tag tag-value]` command.

**Parameters**

<b><i>as number</i></b>	Enter the autonomous system number. The range is from 1 to 65535.
<b><i>metric metric-value</i></b>	(OPTIONAL) Enter the keyword <code>metric</code> then the metric-value number. The range is from 0 to 16777214.
<b><i>metric-type type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: <ul style="list-style-type: none"><li>• 1 = for OSPF External type 1</li><li>• 2 = for OSPF External type 2</li></ul>
<b><i>tag tag-value</i></b>	(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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

# redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

**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**

<b><i>tag</i></b>	(OPTIONAL) Enter the name of the IS-IS routing process.
<b><i>level-1</i></b>	(OPTIONAL) Enter the keywords <code>level-1</code> to redistribute only IS-IS Level-1 routes.
<b><i>level-1-2</i></b>	(OPTIONAL) Enter the keywords <code>level-1-2</code> to redistribute both IS-IS Level-1 and Level-2 routes.
<b><i>level-2</i></b>	(OPTIONAL) Enter the keywords <code>level-2</code> to redistribute only IS-IS Level-2 routes.
<b><i>metric metric-value</i></b>	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 4294967295.
<b><i>metric-type type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: <ul style="list-style-type: none"><li>• 1 = for OSPF External type 1</li><li>• 2 = for OSPF External type 2</li></ul>
<b><i>route-map map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.

**tag tag-value** (OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## router-id

To configure a fixed router ID, use this command.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `router ospf process-id`

To clear an OSPF instance, use the `no router ospf process-id` command.

<b>Parameters</b>	<b><i>process-id</i></b>	Enter a number for the OSPF instance. The range is from 1 to 65535.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF.	
<b>Example</b>	<pre>Dell(conf)#router ospf 2 Dell(conf-router_ospf)#</pre>	

## show config

Display the non-default values in the current OSPF configuration.

<b>Syntax</b>	<code>show config</code>	
<b>Command Modes</b>	ROUTER OSPF	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Example</b>	<pre>Dell(conf-router_ospf)#show config ! router ospf 3 passive-interface FastEthernet 0/1 Dell(conf-router_ospf)#</pre>
----------------	--

## show ip ospf

Display information on the OSPF process configured on the switch.

<b>Syntax</b>	<code>show ip ospf <i>process-id</i></code>	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the `show ip ospf` command shown in the following example.

Line Beginning with	Description
“Routing Process...”	Displays the OSPF process ID and the IP address associated with the process ID.
“Supports only...”	Displays the number of Type of Service (TOS) 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.

<b>Syntax</b>	<code>show ip ospf <i>process-id</i> asbr</code>	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<b>Defaults</b>	none	
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	



<b>Command History</b>	<table border="0"> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>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.</p> <p> <b>NOTE:</b> ASBRs that are not in directly connected areas are also displayed.</p> <p>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 (-/-/-/).</p>						

**Example**

```
Dell#show ip ospf lasbr

RouterID  Flags  Cost  Nexthop  Interface  Area
3.3.3.3   -/-/-/  2     10.0.0.2  Gi 0/1     1
1.1.1.1   E/-/-/  0     0.0.0.0   -          0
Dell#
```

## show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

<b>Syntax</b>	<code>show ip ospf <i>process-id</i> database [database-summary]</code>	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<b><i>database-summary</i></b>	(OPTIONAL) Enter the keywords <code>database-summary</code> to the display the number of LSA types in each area and the total number of LSAs.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<table border="0"> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**Usage Information** The following describes the `show ip ospf process-id database` command shown in the following example.

Field	Description
<b>Link ID</b>	Identifies the router ID.
<b>ADV Router</b>	Identifies the advertising router's ID.
<b>Age</b>	Displays the link state age.
<b>Seq#</b>	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
<b>Checksum</b>	Displays the Fletcher checksum of an LSA's complete contents.
<b>Link count</b>	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.

**Syntax** `show ip ospf process-id database asbr-summary [link-state-id] [adv-router ip-address]`

**Parameters**

- process-id*** Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- link-state-id*** (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network's IP address for Type 3 LSAs or Type 5 LSAs
  - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- adv-router ip-address*** (OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip ospf database asbr-summary` command shown in the following example.

Field	Description
<b>LS Age</b>	Displays the LSA's age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> <li>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li> <li>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li> <li>• E or No E is displayed on whether the originating router can accept AS External LSAs.</li> </ul>
<b>LS Type</b>	Displays the LSA's type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the advertising router's ID.
<b>Checksum</b>	Displays the Fletcher checksum of the LSA's complete contents.
<b>Length</b>	Displays the length in bytes of the LSA.
<b>Network Mask</b>	Displays the network mask implemented on the area.
<b>TOS</b>	Displays the Type of Service (TOS) options. Option 0 is the only option.
<b>Metric</b>	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]
```

<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<b><i>link-state-id</i></b>	(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: <ul style="list-style-type: none"> <li>the network's IP address for Type 3 LSAs or Type 5 LSAs</li> <li>the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs</li> <li>the default destination (0.0.0.0) for Type 5 LSAs</li> </ul>
	<b><i>adv-router ip-address</i></b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip ospf process-id database external` command shown in the following example.

<b>Field</b>	<b>Description</b>
<b>LS Age</b>	Displays the LSA's age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> <li>TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li> <li>DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li> <li>E or No E is displayed on whether the originating router can accept AS External LSAs.</li> </ul>
<b>LS Type</b>	Displays the LSA's type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the router ID of the LSA's originating router.
<b>LS Seq Number</b>	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
<b>Checksum</b>	Displays the Fletcher checksum of the LSA's complete contents.
<b>Length</b>	Displays the length in bytes of the LSA.
<b>Network Mask</b>	Displays the network mask implemented on the area.
<b>Metrics Type</b>	Displays the external type.
<b>TOS</b>	Displays the Type of Service (TOS) options. Option 0 is the only option.
<b>Metric</b>	Displays the LSA metric.
<b>Forward Address</b>	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.
<b>External Route Tag</b>	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** `show ip ospf process-id database network [link-state-id] [adv-router ip-address]`

**Parameters**

- process-id*** Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- link-state-id*** (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network's IP address for Type 3 LSAs or Type 5 LSAs
  - the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- adv-router ip-address*** (OPTIONAL) Enter the keywords `adv-router` and the `ip-address` to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip ospf process-id database network` command shown in the following example.

Field	Description
<b>LS Age</b>	Displays the LSA's age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"> <li>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li> <li>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li> <li>• E or No E is displayed on whether the originating router can accept AS External LSAs.</li> </ul>
<b>LS Type</b>	Displays the LSA's type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the router ID of the LSA's originating router.
<b>Checksum</b>	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
<b>Length</b>	Displays the Fletcher checksum of an LSA's complete contents.
<b>Network Mask</b>	Displays the length in bytes of the LSA.
<b>Attached Router</b>	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 database nssa-external [link-state-id] [adv-router ip-address]`

**Parameters**

***link-state-id*** (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

***adv-router ip-address*** (OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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**

***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` and the ip-address to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show ip ospf process-id database opaque-area` command shown in the following example.

Item	Description
<b>LS Age</b>	Displays the LSA's age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"><li>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li><li>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li><li>• E or No E is displayed on whether the originating router can accept AS External LSAs.</li></ul>
<b>LS Type</b>	Displays the LSA's type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the advertising router's ID.
<b>Checksum</b>	Displays the Fletcher checksum of the LSA's complete contents.
<b>Length</b>	Displays the length in bytes of the LSA.
<b>Opaque Type</b>	Displays the Opaque type field (the first 8 bits of the Link State ID).
<b>Opaque ID</b>	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** `show ip ospf process-id database opaque-as [link-state-id] [adv-router ip-address]`



<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF process ID to show a specific process. If you do not enter the process ID, the command applies only to the first OSPF process.
	<b><i>link-state-id</i></b>	(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: <ul style="list-style-type: none"> <li>the network's IP address for Type 3 LSAs or Type 5 LSAs</li> <li>the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs</li> <li>the default destination (0.0.0.0) for Type 5 LSAs</li> </ul>
	<b><i>adv-router ip-address</i></b>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the ip-address to display only the LSA information about that router.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>EXEC</li> <li>EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">show ip ospf database</a> — displays OSPF database information.	

## show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

<b>Syntax</b>	<code>show ip ospf <i>process-id</i> database opaque-link [<i>link-state-id</i>] [<i>adv-router ip-address</i>]</code>	
<b>Parameters</b>	<b><i>process-id</i></b>	Enter the OSPF process ID to show a specific process. If you do not enter the process ID, the command applies only to the first OSPF process.
	<b><i>link-state-id</i></b>	(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: <ul style="list-style-type: none"> <li>the network's IP address for Type 3 LSAs or Type 5 LSAs</li> <li>the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs</li> <li>the default destination (0.0.0.0) for Type 5 LSAs</li> </ul>
	<b><i>adv-router ip-address</i></b>	(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.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>EXEC</li> <li>EXEC Privilege</li> </ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">show ip ospf database</a> — 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 you do not enter a process ID, the 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` then the IP address of an Advertising Router to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip ospf process-id database router` command shown in the following example.

Item	Description
<b>LS Age</b>	Displays the LSA age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"><li>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li><li>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li><li>• E or No E is displayed on whether the originating router can accept AS External LSAs.</li></ul>
<b>LS Type</b>	Displays the LSA type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the router ID of the LSA's originating router.
<b>LS Seq Number</b>	Displays the link state sequence number. This number detects duplicate or old LSAs.
<b>Checksum</b>	Displays the Fletcher checksum of an LSA's complete contents.
<b>Length</b>	Displays the length in bytes of the LSA.
<b>Number of Links</b>	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
<b>Link connected to:</b>	Identifies the type of network to which the router is connected.
<b>(Link ID)</b>	Identifies the link type and address.
<b>(Link Data)</b>	Identifies the router interface address.

Item	Description
<b>Number of TOS Metric</b>	Lists the number of TOS metrics.
<b>TOS 0 Metric</b>	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**

**process-id** Enter the OSPF process ID to show a specific process. If you do not enter a process ID, the 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` then the IP address of an Advertising Router to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip ospf process-id database summary` command shown in the following example.

Item	Description
<b>LS Age</b>	Displays the LSA age.
<b>Options</b>	Displays the optional capabilities available on router. The following options can be found in this item: <ul style="list-style-type: none"><li>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</li><li>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</li><li>• E or No E is displayed on whether the originating router can accept AS External LSAs.</li></ul>
<b>LS Type</b>	Displays the LSA type.
<b>Link State ID</b>	Displays the Link State ID.
<b>Advertising Router</b>	Identifies the router ID of the LSA's originating router.
<b>LS Seq Number</b>	Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.
<b>Checksum</b>	Displays the Fletcher checksum of an LSA's complete contents.
<b>Length</b>	Displays the length in bytes of the LSA.
<b>Network Mask</b>	Displays the network mask implemented on the area.
<b>TOS</b>	Displays the TOS options. Option 0 is the only option.
<b>Metric</b>	Displays the LSA metrics.

## Example

```
#show ip ospf 100 database summary
```

```

OSPF Router with ID (1.1.1.10) (Process ID 100)

    Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
    TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
Network Mask: /24
    TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
    TOS: 0 Metric: 1

#

```

### Related Commands

[show ip ospf database](#) — displays OSPF database information.

## show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

**Syntax** `show ip ospf process-id interface [interface]`

### Parameters

- process-id*** Enter the OSPF process ID to show a specific process. If you do not enter a process ID, the command applies only to the first OSPF process.
- interface*** (OPTIONAL) Enter the following keywords and slot/port or number information:
- For the null interface, enter the keyword `null` then zero (0).
  - For Loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383.
  - For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The following describes the `show ip ospf process-id interface` command shown in the following example.

Item	Description
<b>TenGigabitEthernet net...</b>	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
<b>Internet Address...</b>	This line displays the IP address, network mask and area assigned to this interface.
<b>Process ID...</b>	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
<b>Transmit Delay...</b>	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
<b>Designated Router...</b>	This line displays the ID of the Designated Router and its interface address.
<b>Backup Designated...</b>	This line displays the ID of the Backup Designated Router and its interface address.
<b>Timer intervals...</b>	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
<b>Hello due...</b>	This line displays the amount time until the next Hello packet is sent out this interface.
<b>Neighbor Count...</b>	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 1/1 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 1/2 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** *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.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip ospf process-id neighbor` command shown in the following example.

Item	Description
<b>Neighbor ID</b>	Displays the neighbor router ID.
<b>Pri</b>	Displays the priority assigned neighbor.
<b>State</b>	Displays the OSPF state of the neighbor.
<b>Dead Time</b>	Displays the expected time until the system declares the neighbor dead.
<b>Address</b>	Displays the IP address of the neighbor.
<b>Interface</b>	Displays the interface type slot/port information.
<b>Area</b>	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 Gi 0/0 0.0.0.2
192.10.10.2 1 FULL/DR      00:00:37 192.10.10.2 Gi 0/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER 00:00:36 192.10.10.4 Gi 0/1 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

This command is useful in isolating routing problems between the OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

### Example

```
Dell#show ip ospf 100 route

Prefix          Cost Nexthop   Interface Area  Type
1.1.1.1         1   0.0.0.0    Lo 0     0    Intra-Area
3.3.3.3         2   13.0.0.3   Te 0/4   1    Intra-Area
13.0.0.0        1   0.0.0.0    Te 0/4   0    Intra-Area
150.150.150.0   2   13.0.0.3   Te 0/4   -    External
172.30.1.0      2   13.0.0.3   Te 0/4   1    Intra-Area
Dell#
```

## show ip ospf statistics

Display OSPF statistics.

**Syntax** `show ip ospf process-id statistics global | [interface name {neighbor router-id}]`

Parameters	
<b><i>process-id</i></b>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<b>global</b>	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.
<b><i>interface name</i></b>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For Port Channel groups, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
<b><i>neighbor router-id</i></b>	(OPTIONAL) Enter the keyword <code>neighbor</code> then the neighbor's router-id in dotted decimal format (A.B.C.D.).

**Defaults** none

**Supported Modes** Full-Switch

- Command Modes**
- EXEC
  - EXEC Privilege

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip ospf statistics process-id global` command shown in the following example.



Row Heading	Description
<b>Total</b>	Displays the total number of packets the OSPF process receives/transmits.
<b>Error</b>	Displays the error count while receiving and transmitting packets by the OSPF process.
<b>Hello</b>	Number of OSPF Hello packets.
<b>DDiscr</b>	Number of database description packets.
<b>LSReq</b>	Number of link state request packets.
<b>LSUpd</b>	Number of link state update packets.
<b>LSAck</b>	Number of link state acknowledgement packets.
<b>TxQ-Len</b>	The transmission queue length.
<b>RxQ-Len</b>	The reception queue length.
<b>Tx-Mark</b>	The highest number mark in the transmission queue.
<b>Rx-Mark</b>	The highest number mark in the reception queue.
<b>Hello-Q</b>	The queue, for transmission or reception, for the hello packets.
<b>LSR-Q</b>	The queue, for transmission or reception, for the link state request packets.
<b>Other-Q</b>	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
<b>Intf_Down</b>	Received packets on an interface that is either down or OSPF is not enabled.
<b>Non-Dr</b>	Received packets with a destination address of ALL_DRS even though SELF is not a designated router.
<b>Self-Org</b>	Receive the self originated packet.
<b>Wrong_Len</b>	The received packet length is different to what was indicated in the OSPF header.
<b>Invlid-Nbr</b>	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.
<b>Nbr-State</b>	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.
<b>Auth-Error</b>	Simple authentication error.
<b>MD5-Error</b>	MD5 error
<b>Cksum-Err</b>	Checksum Error
<b>Version</b>	Version mismatch
<b>AreaMismatch</b>	Area mismatch
<b>Conf-Issue</b>	The received hello packet has a different hello or dead interval than the configuration.
<b>No-Buffer</b>	Buffer allocation failure.
<b>Seq-no</b>	A sequence no errors occurred during the database exchange process.
<b>Socket</b>	Socket Read/Write operation error.
<b>Q-overflow</b>	Packets dropped due to queue overflow.
<b>Unknown-Pkt</b>	Received packet is not an OSPF packet.

### Example

```
Dell#show ip ospf 10 statistics global
```

```

    OSPF Packet Count
      Total Error Hello DDiscr LSReq LSUpd
LSAck
RX          34      0    26      2      1      3
2
TX          34      0    25      3      1      3
2

    OSPF Global Queue Length
      TxQ-Len RxQ-Len Tx-Mark Rx-Mark
Hello-Q          0      0      1      1
LSR-Q            0      0      1      1
Other-Q          0      0      2      2

    Error packets (Receive statistics)
Intf-Down    0 Non-Dr      0 Self-Org 0
Wrong-Len    0 InvlD-Nbr  0 Nbr-State
0
Auth-Err     0 MD5-Err     0 Chksum 0
Version      0 AreaMis     0 Conf-Issues
0
No-Buffer    0 Seq-No      0 Socket 0
Q-OverFlow   0 Unknown-Pkt 0 RtidZero
0
Error packets (Transmit statistics)
Socket Errors 0
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#show ip ospf 10 statistics
Interface TenGigabitEthernet 4/45
  Error packets (Receive statistics)
    Intf-Down    0 Non-Dr      0 Self-Org    0
    Wrong-Len    0 InvlD-Nbr  0 Nbr-State   0
    Auth-Error   0 MD5-Error   0 Cksum-Err   0
    Version      0 AreaMisMatch 0 Conf-Issue  0
    SeqNo-Err    0 Unknown-Pkt 0 Bad-LsReq  0
    RtidZero     0
  Neighbor ID 3.1.1.2
  Packet Statistics
    Hello DDiscr LSReq LSUpd LSAck
    RX      47      2      1      3      2
    TX      46      3      1      3      2
  Timers
    Hello      1 Wait          0      Grace 0
    Dead      37 Transmit      0
  Queue Statistics
    LSU-Q-Len  0 LSU-Q-Wmark  1
    LSR-Q-Len  0 LSR-Q-Wmark  1
Dell#

```

### 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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** *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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

## Example

```
Dell#show ip ospf 1 topology

Router ID  Flags Cost  Nexthop  Interface Area
3.3.3.3    E/B/-/  1        20.0.0.3 Te 0/6    0
1.1.1.1    E/-/-/  1        10.0.0.1 Te 0/6    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**

- ip-address** Specify the IP address in dotted decimal format of the address to summarize.
- mask** Specify the mask in dotted decimal format of the address to summarize.
- not-advertise** (OPTIONAL) Enter the keywords `not-advertise` to suppress that match the network prefix/mask pair.
- tag tag-value** (OPTIONAL) Enter the keyword `tag` then a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The `area range` command summarizes routes for the different areas.

With the `not-advertise` parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0, you can configure the `summary-address 1.1.0.0 255.255.0.0 not-advertise` to filter out all the routes fall in range 1.1.0.0/16.


**Related Commands** [area range](#) — summarizes routes within an area.

# timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

**Syntax** `timers spf delay holdtime msec`  
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 2147483647. The default is **5 seconds**.
- holdtime** Enter a number as the hold time. The range is from 0 to 2147483647. The default is **10 seconds**.
- msec** Enter the keyword `msec` to specify the time interval value in milli seconds.  
 **NOTE:** If you do not specify the msec option, the timer values are considered as seconds.

**Defaults**

- delay = 5 seconds
- holdtime = 10 seconds

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.11(0.0)</b></td> <td>Introduced the <code>msec</code> keyword.</td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.11(0.0)</b>	Introduced the <code>msec</code> keyword.	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description								
<b>9.11(0.0)</b>	Introduced the <code>msec</code> keyword.								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.								
<b>Usage Information</b>	Setting the <i>delay</i> and <i>holdtime</i> parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.								

**Example for IPv4 and IPv6**

```
Dell#
Dell#conf
Dell(conf)#router ospf 1
Dell(conf-router_ospf-1)#timer spf 2 5 msec
Dell(conf-router_ospf-1)#
Dell(conf-router_ospf-1)#show config
!
router ospf 1
timers spf 2 5 msec
Dell(conf-router_ospf-1)#
Dell(conf-router_ospf-1)#end
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

**Supported Modes** Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

**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** `timers throttle lsa arrival arrival-time`  
To return to the default, use the `no timers throttle lsa` command.

**Parameters** *arrival-time* Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is from 0 to 600,000 milliseconds.

**Defaults** 1000 msec

**Command Modes** ROUTER OSPF

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## OSPFv3 Commands

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

## area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OSPFv3 area.

**Syntax** `area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key`

Parameters	Description
<i>area area-id</i>	Area for which OSPFv3 traffic is to be authenticated. For <i>area-id</i> , you can enter a number. The range is from 0 to 4294967295.
<i>ipsec spi number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
<b>MD5   SHA1</b>	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
<b>key-encryption-type</b>	(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).
<b>key</b>	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

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## 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 | null
```

To remove an IPsec encryption policy from an interface, use the `no area area-id encryption spi number` command.

**Parameters**

<b>area <i>area-id</i></b>	Area for which OSPFv3 traffic is to be encrypted. For <i>area-id</i> , enter a number. The range is from 0 to 4294967295.
<b>ipsec spi <i>number</i></b>	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
<b>esp encryption-algorithm</b>	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.
<b>key-encryption-algorithm</b>	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<b>key</b>	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.
<b>authentication-algorithm</b>	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.
<b>key-encryption-type</b>	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<b>key</b>	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

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## area nssa

Specify an area as a not so stubby area (NSSA).

**Syntax** `area area-id nssa [default-information-originate] [no-redistribution] [no-summary]`

To delete an NSSA, use the `no area area-id nssa` command.

**Parameters**

<b>area-id</b>	Specify the OSPF area by entering a number from zero (0) to 65535.
<b>no-redistribution</b>	(OPTIONAL) Specify that the <code>redistribute</code> command does not distribute routes into the NSSA. This command can be used when the router is an autonomous system boundary router (ASBR) or area border router (ABR).
<b>default-information-originate</b>	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
<b>no-summary</b>	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

**Defaults** Not configured.

**Command Modes** ROUTER OSPF

**Command History**

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



Version	Description
9.13(0.0)	Introduced on the remaining DNOS platforms.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

## auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

**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 ref-bw]` command.

**Parameters** `ref-bw` (OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is **100 megabits per second**.

**Defaults** **100 megabits per second.**

**Command Modes** ROUTER OSPFv3

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM
9.9(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

## Example

```
Dell#show running-config ospf
!
ipv6 router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 2000

Dell(conf-ipv6-router_ospf)#auto-cost reference-bandwidth ?
<1-4294967>          Reference bandwidth in Mbits/second (default =
100)
Dell(conf-ipv6-router_ospf)#no auto-cost ?
reference-bandwidth  Use reference bandwidth method to assign OSPF
cost
<cr>
Dell(conf-ipv6-router_ospf)#
```

## clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

**Syntax** `clear ipv6 ospf process`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

## debug ipv6 ospf

Display debug information and interface types on OSPF IPv6 packets or events.

**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 information.
- For a Port Channel interface, enter the keyword `port-channel` then a number. The range is 1 to 128.
- For a tunnel interface, enter the keyword `tunnel` then a number. The range is 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

# debug ipv6 ospf bfd

Display debug information and interface types for BFD on OSPF IPv6 packets.

**Syntax** [no] debug ipv6 ospf bfd [*interface*]

To cancel the debug command, use the no debug ipv6 ospf command.

**Parameters** *interface* (OPTIONAL) Enter one of the following keywords and slot/port or number information:

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

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following section describes the command fields.

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..

## Example

```
Dell(conf-if-te-0/2)#do debug ipv6 ospf bfd te 0/2
OSPFv3 bfd related debugging is on for TenGigabitEthernet 0/2
00:59:26 : OSPFv3INFO: Received Interface mode bfd config command on
interface Te 0/2 Enable 1, interval 0, min_rx 0, Multiplier 0, role 0,
Disable 0
00:59:26 : OSPFv3INFO: Enabling BFD on interface Te 0/2 Cmd Add Session
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Completed Enabling BFD on interface Te 0/2
00:59:27 : OSPFv3INFO: Completed Interface mode BFD configuration on Te
0/2!!
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Ospf3_register_bfd ospf key 27648
00:59:27 : OSPFv3INFO: OSPFV3 Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720 Interface Te 0/2 IfIndex 34145282
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3
role active
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3
role active
00:59:27 : OSPFv3INFO: Completed Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
Aug 25 11:19:59: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed
session state to Init for neighbor fe80::201:e8ff:fe8b:7720 on interface
```

```

Te 0/2 (diag: NBR_DN)
Aug 25 11:20:00: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed
session state to Up for neighbor fe80::201:e8ff:fe8b:7720 on interface
Te 0/2 (diag: NO_DIAG)
00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg
00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Te 0/2
00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state

```

## debug ipv6 ospf events

Display debug information and interface types on OSPF IPv6 events.

**Syntax** `debug ipv6 ospf events [interface] [vrf vrf-name]`

**Parameters**

**interface** (OPTIONAL) Enter one of the following keywords and slot/port or number information:

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

**vrf vrf-name** Enter the keyword `vrf` to view debugging information on OSPF corresponding to that VRF.

**Command Modes** EXEC Privilege

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

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on E-Series.

**Example**

**Example (detail)**

Command Fields	Lines	Description
	<b>Beginning With or Including</b>	
	<b>OSPFv3...</b>	Debugging is on for all OSPFv3 packets and all interfaces.
	<b>05:21:01</b>	Displays the time stamp.
	<b>Sending Ver:3</b>	Sending OSPF3 version..
	<b>type:</b>	Displays the type of packet sent: <ul style="list-style-type: none"> <li>• 1 - Hello packet</li> <li>• 2 - database description</li> <li>• 3 - link state request</li> <li>• 4 - link state update</li> <li>• 5 - link state acknowledgement</li> </ul>
	<b>Length:</b>	Displays the OSPFv3 packet length.
	<b>Router ID:</b>	Displays the OSPFv3 router ID.
	<b>Area ID:</b>	Displays the OSPFv3 area ID.
	<b>Chksum:</b>	Displays the OSPFv3 checksum.

## debug ipv6 ospf packet

Display debug information and interface types on OSPF IPv6 packets.

**Syntax** `debug ipv6 ospf packet [interface] [vrf vrf-name] [detail]`

Parameters		
<b>interface</b>	(OPTIONAL) Enter one of the following keywords and slot/port or number information:	<ul style="list-style-type: none"> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.</li> <li>• For a port channel interface, enter the keywords <code>port-channel</code> then a number.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
<b>vrf vrf-name</b>	Enter the keyword <code>vrf</code> to view debugging information on OSPF corresponding to that VRF.	
<b>detail</b>	Enter the keyword <code>detail</code> to view detailed debugging information.	

**Command Modes** EXEC Privilege

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

Version	Description
<b>9.14.1.0</b>	The <code>detail</code> option is introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Added support for detailed debugging.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the S6100-ON.
<b>9.8(2.0)</b>	Introduced on the S3100 series.

Version	Description
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on E-Series.

### Example

#### Example (detail)

#### Command Fields

Lines	Description
<b>Beginning With or Including</b>	
<b>OSPFv3...</b>	Debugging is on for all OSPFv3 packets and all interfaces.
<b>05:21:01</b>	Displays the time stamp.
<b>Sending Ver:3</b>	Sending OSPF3 version..
<b>type:</b>	Displays the type of packet sent: <ul style="list-style-type: none"> <li>• 1 - Hello packet</li> <li>• 2 - database description</li> <li>• 3 - link state request</li> <li>• 4 - link state update</li> <li>• 5 - link state acknowledgement</li> </ul>
<b>Length:</b>	Displays the OSPFv3 packet length.
<b>Router ID:</b>	Displays the OSPFv3 router ID.
<b>Area ID:</b>	Displays the OSPFv3 area ID.
<b>Chksum:</b>	Displays the OSPFv3 checksum.

## debug ipv6 ospf spf

Display debug information for SPF timers on OSPF IPv6 packets.

**Syntax** [no] debug ipv6 ospf spf [vrf vrf-name]

**Parameters** *interface* (OPTIONAL) Enter one of the following keywords and slot/port or number information:

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

**vrf *vrf-name*** Enter the keyword `vrf` to view debugging information on OSPF corresponding to that VRF.

**Command Modes** EXEC Privilege

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

Version	Description
9.11.0.0	Introduced the command.

**Usage Information** The following section describes the command fields.

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..

### Example

## default-information originate

Configure the system to generate a default external route into an OSPFv3 routing domain.

**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**

<b>always</b>	(OPTIONAL) Enter the keyword <code>always</code> to specify that default route information must always be advertised.
<b>metric <i>metric-value</i></b>	(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.
<b>metric-type <i>type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then an OSPFv3 link state type of 1 or 2 for default routes. The values are: <ul style="list-style-type: none"><li>• 1 = Type 1 external route</li><li>• 2 = Type 2 external route</li></ul>
<b>route-map <i>map-name</i></b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of an established route map.

**Defaults** Disabled.

**Command Modes** ROUTER OSPFv3

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

# 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.

<b>Syntax</b>	<code>graceful-restart grace-period seconds</code> To disable OSPFv3 graceful restart, enter <code>no graceful-restart grace-period</code> .						
<b>Parameters</b>	<b>seconds</b> 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.						
<b>Defaults</b>	OSPFv3 graceful restart is disabled and functions in a helper-only role.						
<b>Command Modes</b>	ROUTER OSPFv3						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.						

**Usage Information**

By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

To enable OSPFv3 graceful restart, enter the `ipv6 router ospf` command to enter OSPFv3 configuration mode and then configure a grace period using the `graceful-restart grace-period` command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link.

When you enable the helper-reject role on an interface with the `ipv6 ospf graceful-restart helper-reject` command, you reconfigure OSPFv3 graceful restart to function in a “restarting-only” role. In a “restarting-only” role, OSPFv3 does not participate in the graceful restart of a neighbor.

# graceful-restart mode

Specify the type of events that trigger an OSPFv3 graceful restart.

<b>Syntax</b>	<code>graceful-restart mode {planned-only   unplanned-only}</code> To disable graceful restart mode, enter <code>no graceful-restart mode</code> .						
<b>Parameters</b>	<b>planned-only</b> (OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only. <b>unplanned-only</b> (OPTIONAL) Enter the keywords <code>unplanned-only</code> to indicate graceful restart is supported in an unplanned restart condition only.						
<b>Defaults</b>	OSPFv3 graceful restart supports both planned and unplanned failures.						
<b>Command Modes</b>	ROUTER OSPFv3						
<b>Supported Modes</b>	Full—Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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**

**process-id** Enter the process identification number.

**area area-id** Specify the OSPF area. The range is from 0 to 4294967295.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.14(0.2)</b>	Increased the area ID value from 65535 to 4294967295.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 ospf authentication

Enable IPv6 OSPF on an interface.

**Syntax** `ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} [key-encryption-type] key}`

To remove an IPsec authentication policy from an interface, use 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, use the `no ipv6 ospf authentication null` command.

**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

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

**Syntax**

```
ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command.

**Parameters**

**disable**

(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.

**interval  
milliseconds**

(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100.

**min\_rx  
milliseconds**

Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 100. The default is **100**.

**multiplier *value***

Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

**role [active |  
passive]**

Enter the role that the local system assumes:

- **active** — The active system initiates the BFD session. Both systems can be active for the same session.
- **passive** — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

**Defaults** See Parameters.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

Version	Description
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure the `ipv6 ospf bfd` command in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configured BFD in CONFIGURATION mode.

To disable BFD on a specific interface while BFD is configured in CONFIGURATION mode, use the keyword `disable`.

## 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

**Supported Modes** Full—Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

In general, the path cost is calculated as:

$10^8 / \text{bandwidth}$

Using this formula, the default path cost is calculated as:

- TenGigabitEthernet—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`

**Parameters** *seconds* Enter the time interval in seconds. The range is from 1 to 65535 seconds.

**Defaults** 40 seconds (Ethernet).

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

By default, the dead interval is four times longer than the default `ipv6 ospf hello-interval` command.

# 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}
```

To remove an IPsec encryption policy from an interface, use 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, use the `no ipv6 ospf encryption null` command.

## Parameters

<b>null</b>	Causes an encryption policy configured for the area to not be inherited on the interface.
<b>ipsec spi number</b>	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
<b>esp encryption-algorithm</b>	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.
<b>key-encryption-type</b>	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<b>key</b>	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.
<b>authentication-algorithm</b>	Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.
<b>key-encryption-type</b>	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
<b>key</b>	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

**Supported Modes** Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

# 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, use the `no ipv6 ospf graceful-restart helper-reject` command.

**Defaults** The helper-reject role is not configured.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Command** 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`

**Parameters** *seconds* Enter the time interval in seconds as the time between hello packets. The range is from 1 to 65525 seconds.

**Defaults** 10 seconds (Ethernet).

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The time interval between hello packets must be the same for routers in a network.

## ipv6 ospf priority

To determine the Designated Router for the OSPFv3 network, set the priority of the interface.

<b>Syntax</b>	<code>ipv6 ospf priority <i>number</i></code> To return to the default time interval, use the <code>no ipv6 ospf priority</code> command.						
<b>Parameters</b>	<b><i>number</i></b> Enter the number as the priority. The range is from 1 to 255.						
<b>Defaults</b>	1						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ipv6 router ospf <i>process-id</i></code> To exit OSPF for IPv6, use the <code>no ipv6 router ospf <i>process-id</i></code> command.						
<b>Parameters</b>	<b><i>process-id</i></b> Enter the process identification number. The range is from 1 to 65535.						
<b>Defaults</b>	none						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.						

## maximum-paths

Enable the software to forward packets over multiple paths.

<b>Syntax</b>	<code>maximum-paths <i>number</i></code> To disable packet forwarding over multiple paths, use the <code>no maximum-paths</code> command.
<b>Parameters</b>	<b><i>number</i></b> Specify the number of paths. The range is from 1 to 64. The default is <b>8</b> paths.
<b>Defaults</b>	4
<b>Command Modes</b>	ROUTER OSPF for OSPFv3

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Added support for OSPFv3.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## passive-interface

Disable (suppress) sending routing updates on an interface.

**Syntax** `passive-interface {default | interface}`

To enable sending routing updates on an interface, 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**

<b>Default</b>	Enter the keyword <code>default</code> to make all OSPF interfaces (current and future) passive.
<b>interface</b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>

**Command Modes** ROUTER OSPF for OSPFv2  
ROUTER OSPFv3 for OSPFv3

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Added support for OSPFv3.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

By default, no interfaces are *passive*. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

## redistribute

Redistribute information from another routing protocol into OSPFv3 throughout the OSPF process.

**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

<b>bgp <i>as number</i></b>	Enter the keyword <code>bgp</code> then the autonomous system number. The range is from 1 to 65535.
<b>connected</b>	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
<b>static</b>	Enter the keyword <code>static</code> to redistribute manually configured routes.
<b>metric <i>metric-value</i></b>	Enter the keyword <code>metric</code> then the metric value. The range is from 0 to 16777214. The default is <b>20</b> .
<b>metric-type <i>type-value</i></b>	(OPTIONAL) Enter the keywords <code>metric-type</code> then the OSPFv3 link state type of 1 or 2 for default routes. The values are: <ul style="list-style-type: none"><li>• 1 for a type 1 external route</li><li>• 2 for a type 2 external route</li></ul> The default is <b>2</b> .
<b>route-map <i>map-name</i></b>	(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 <b>deny</b> (to drop all routes).
<b>tag <i>tag-value</i></b>	(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 <b>0</b> .

**Defaults** Not configured.

**Command Modes** ROUTER OSPF for OSPFv2  
ROUTER OSPFv3 for OSPFv3

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Added support for OSPFv3.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To redistribute the default route (x:x:x:x), use the `default-information originate` command.

**Related Commands** [default-information originate](#) — generates a default route into the OSPF routing domain.

## 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.



<b>Parameters</b>	<b><i>ip-address</i></b>	Enter the router ID in the dotted decimal format.
<b>Defaults</b>	The router ID is selected automatically from the set of IPv4 addresses configured on a router.	
<b>Command Modes</b>	ROUTER OSPFv3 for OSPFv3	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Added support for OSPFv3.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.</p> <p>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.</p>	

#### 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#
```

## show crypto ipsec policy

Display the configuration of IPsec authentication and encryption policies.

<b>Syntax</b>	<b>show crypto ipsec policy</b> [ <i>name name</i> ]	
<b>Parameters</b>	<b>name <i>name</i></b>	(OPTIONAL) Displays configuration details about a specified policy.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>The <code>show crypto ipsec policy</code> command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.</p> <p>When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.</p>	

# show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

<b>Syntax</b>	<code>show crypto ipsec sa ipv6 [interface <i>interface</i>]</code>	
<b>Parameters</b>	<b>interface</b> <b><i>interface</i></b>	(OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where <i>interface</i> is one of the following values: <ul style="list-style-type: none"><li>• For a Port Channel interface, enter <code>port-channel</code> then the port channel number.</li><li>• For a 10-Gigabit Ethernet interface, enter <code>TenGigabitEthernet</code> then the slot/port number.</li><li>• For a VLAN interface, enter <code>vlan <i>vlan-id</i></code>. The valid VLAN IDs range is from 1 to 4094.</li></ul>
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.	

# show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

<b>Syntax</b>	<code>show ipv6 ospf database [database-summary   grace-lsa]</code>	
<b>Parameters</b>	<b>database-summary</b>	(OPTIONAL) Enter the keywords <code>database-summary</code> to view a summary of database LSA information.
	<b>grace-lsa</b>	(OPTIONAL): Enter the keywords <code>grace-lsa</code> to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>Usage Information</b>	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.	

## show ipv6 ospf interface

View OSPFv3 interface information.

**Syntax** `show ipv6 ospf [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` and the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` and a number. The range is from 1 to 128.
- For a Tunnel interface, enter the keywords `tunnel` and a number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` and a number from 1 to 4094.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**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 interface Tengigabitethernet 1/0

TengigabitEthernet 1/0 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 neighbor [interface]`

**Parameters** **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 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 the VLAN ID. The range is 1 to 4094.

**Defaults** none

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

## snmp context

Configure SNMPv3 context name to map multiple OSPFv3 VRF instances.

**Syntax** `snmp context {context-name}`  
To clear snmp context, use the `no snmp context {context-name}` command.

**Parameters** **context-name** Enter the SNMP context name. The maximum length is 32 alphanumeric characters.

**Defaults** None.

**Command Modes** IPv6 ROUTER OSPF

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, Z9500, S6000-ON, C9010, MXL, and FN IOM.

**Usage Information** Use SNMPv3 context configuration to distinguish between various OSPFv3 VRF instances.

### Example

```
DellEMC(conf-ipv6-router_ospf)#snmp context ospf1
```

```
DellEMC>show runnig-config ospf
!
ipv6 router ospf 10
router-id 10.10.10.1
snmp context ospf1
!
DellEMC>
```

## timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

**Syntax** `timers spf delay holdtime msec`  
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 2147483647. The default is **5 seconds**.  
**holdtime** Enter a number as the hold time. The range is from 0 to 2147483647. The default is **10 seconds**.

**msec**

Enter the keyword `msec` to specify the time interval value in milli seconds.

**NOTE:** If you do not specify the `msec` option, the timer values are considered as seconds.

**Defaults**

- delay = 5 seconds
- holdtime = 10 seconds

**Command Modes** ROUTER OSPFv3 for OSPFv3

**Supported Modes** Full-Switch

**Command History**

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

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

Version	Description
<b>9.11(0.0)</b>	Introduced the <code>msec</code> keyword.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.8(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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)#ipv6 router ospf 1
Dell(conf-ipv6-router_ospf)#timer spf 2 5 msec
Dell(conf-ipv6-router_ospf)#
Dell(conf-ipv6-router_ospf)#show config
!
ipv6 router ospf 1
timers spf 2 5 msec
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 software (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.

## Topics:

- [description](#)
- [ip redirect-group](#)
- [ip redirect-list](#)
- [permit](#)
- [redirect](#)
- [seq](#)
- [show cam pbr](#)
- [show ip redirect-list](#)

## description

Add a description to this redirect list.

**Syntax** `description {description}`  
To remove the description, use the `no description {description}` command.

**Parameters** *description* Enter a description to identify the IP redirect list (16 characters maximum).

**Defaults** none

**Command Modes** REDIRECT-LIST

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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-nametext [l2-switch]`  
To remove a redirect list from an interface, use the `no ip redirect-group name` command.

<b>Parameters</b>	<b><i>redirect-list-name</i></b>	Enter the name of a configured redirect list.
	<b>l2-switch</b>	Enter the keyword <code>l2-switch</code> to enable PBR on Layer2 (switched) traffic.

**Defaults** none

**Command Modes** INTERFACE (conf-if-vl-)

**Supported Modes** Full—Switch


**Command History**

<b>Version</b>	<b>Description</b>
<b>9.11(2.0)</b>	Introduced the <code>l2-switch</code> attribute.
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>8.4.2.1</b>	Introduced on the C-Series and S-Series.
<b>8.4.2.0</b>	Introduced on the E-Series TeraScale.
<b>7.4.2.0</b>	Added support for LAG and VLAN interfaces.
<b>7.7.1.0</b>	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.

The Layer2 PBR option matches the layer2 traffic flow. If you un-configure this option, then the Layer2 traffic is not matched. You can apply the `l2-switch` option to redirect Layer2 traffic only on a VLAN interface. This VLAN interface must be configured with an IP address for ARP resolution.

 **NOTE:** The `l2-switch` option that redirects Layer2 traffic is applicable only on VLAN interfaces.

The Layer3 routing is not affected on the same interface on which Layer2 PBR is applied. The port from which Layer2 packets egress and the destination MAC are re-written from static ARP. Layer 2 packets with the re-written destination MAC are forwarded through the outgoing port on the same incoming VLAN interface. The `layer2-switch` option ensures that the outgoing VLAN and MAC-SA are changed and TTL is not decremented.

**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** ***redirect-list-name*** Enter the name of a redirect list.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>8.4.2.1</b>	Introduced on the C-Series and S-Series.
	<b>8.4.2.0</b>	Introduced on the E-Series TeraScale.
	<b>6.5.3.0</b>	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** `permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]`

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq sequence-number` syntax command.
- You can also use the `no permit {ip-protocol-number | protocol-type} {source mask | any | host ip-address} {destination mask | any | host ip-address} [bit] [operators]` command.

<b>Parameters</b>	
<b><i>ip-protocol-number</i></b>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<b><i>protocol-type</i></b>	Enter one of the following keywords as the protocol type: <ul style="list-style-type: none"><li>• <code>icmp</code> for internet control message protocol</li><li>• <code>ip</code> for any internet protocol</li><li>• <code>tcp</code> for transmission control protocol</li><li>• <code>udp</code> for user datagram protocol</li></ul>
<b><i>source mask</i></b>	Enter the IP address of the network or host from which the packets were sent.
<b><i>mask</i></b>	Enter a network mask in /prefix format (/x).
<b><i>any</i></b>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<b><i>host ip-address</i></b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b><i>destination</i></b>	Enter the IP address of the network or host to which the packets are sent.
<b><i>bit</i></b>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none"><li>• <code>ack</code> = acknowledgement</li><li>• <code>fin</code> = finish (no more data from the user)</li><li>• <code>push</code> = push function</li><li>• <code>rst</code> = reset the connection</li><li>• <code>syn</code> = synchronize sequence number</li><li>• <code>urg</code> = urgent field</li></ul>
<b><i>operator</i></b>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: <ul style="list-style-type: none"><li>• <code>eq</code> = equal to</li><li>• <code>neq</code> = not equal to</li><li>• <code>gt</code> = greater than</li><li>• <code>lt</code> = less than</li></ul>



- `range` = inclusive range of ports (you must specify two ports for the `portcommand` parameter.)

<b>Defaults</b>	none
<b>Command Modes</b>	REDIRECT-LIST
<b>Supported Modes</b>	Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>8.4.2.1</b>	Introduced on the C-Series and S-Series.
	<b>8.4.2.0</b>	Introduced on the E-Series TeraScale.
	<b>7.5.1.0</b>	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		
<b><i>ip-address</i></b>		Enter the IP address of the forwarding router.
<b><i>slot/port</i></b>		Enter the keyword <code>slot / port</code> followed by the slot/port information.
<b><i>ip-protocol-number</i></b>		Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<b><i>tunnel</i></b>		Enter the keyword <code>tunnel</code> to configure the tunnel setting.
<b><i>tunnel-id</i></b>		Enter the keyword <code>tunnel-id</code> to redirect the traffic.
<b><i>track</i></b>		Enter the keyword <code>track</code> to enable the tracking.
<b><i>track &lt;obj-id&gt;</i></b>		Enter the keyword <code>track &lt;obj-id&gt;</code> to track object-id.
<b><i>protocol-type</i></b>		Enter one of the following keywords as the protocol type: <ul style="list-style-type: none"> <li>• <code>icmp</code> for internet control message protocol</li> <li>• <code>ip</code> for any internet protocol</li> <li>• <code>tcp</code> for transmission control protocol</li> <li>• <code>udp</code> for user datagram protocol</li> </ul>
<b><i>bit</i></b>		(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none"> <li>• <code>ack</code> = acknowledgement</li> <li>• <code>fin</code> = finish (no more data from the user)</li> <li>• <code>push</code> = push function</li> <li>• <code>rst</code> = reset the connection</li> <li>• <code>syn</code> = synchronize sequence number</li> <li>• <code>urg</code> = urgent field</li> </ul>

<b>source</b>	Enter the IP address of the network or host from which the packets were sent.
<b>mask</b>	Enter a network mask in /prefix format (/x).
<b>any</b>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<b>host ip-address</b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b>destination</b>	Enter the IP address of the network or host to which the packets are sent.
<b>operator</b>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: <ul style="list-style-type: none"> <li>• <code>eq</code> = equal to</li> <li>• <code>neq</code> = not equal to</li> <li>• <code>gt</code> = greater than</li> <li>• <code>lt</code> = less than</li> <li>• <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command parameter.)</li> </ul>

<b>Defaults</b>	none
<b>Command Modes</b>	REDIRECT-LIST
<b>Supported Modes</b>	Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Added the keyword <code>track-id</code> on the MXL.
	<b>9.4(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
	<b>8.4.2.1</b>	Introduced on the C-Series.
	<b>8.4.2.0</b>	Introduced on the E-Series TeraScale.

## 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	
<b>sequence-number</b>	Enter a number from 1 to 65535.
<b>permit</b>	Enter the keyword <code>permit</code> assign the sequence to the permit list.
<b>redirect</b>	Enter the keyword <code>redirect</code> to assign the sequence to the redirect list.
<b>ip-address</b>	Enter the IP address of the forwarding router.
<b>tunnel</b>	Enter the keyword <code>tunnel</code> to configure the tunnel setting.
<b>tunnel-id</b>	Enter the keyword <code>tunnel-id</code> to redirect the traffic.
<b>track</b>	Enter the keyword <code>track</code> to enable the tracking.
<b>track &lt;obj-id&gt;</b>	Enter the keyword <code>track &lt;obj-id&gt;</code> to track object-id.

<b><i>ip-protocol-number</i></b>	Enter the keyword <code>ip-protocol-number</code> then the number from 0 to 255 for the protocol identified in the IP protocol header.
<b><i>protocol-type</i></b>	Enter one of the following keywords as the protocol type: <ul style="list-style-type: none"> <li>• <code>icmp</code> for internet control message protocol</li> <li>• <code>ip</code> for any internet protocol</li> <li>• <code>tcp</code> for transmission control protocol</li> <li>• <code>udp</code> for user datagram protocol</li> </ul>
<b><i>source</i></b>	Enter the IP address of the network or host from which the packets were sent.
<b><i>mask</i></b>	Enter a network mask in /prefix format (/x).
<b><i>any</i></b>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<b><i>host ip-address</i></b>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<b><i>destination</i></b>	Enter the IP address of the network or host to which the packets are sent.
<b><i>bit</i></b>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: <ul style="list-style-type: none"> <li>• <code>ack</code> = acknowledgement</li> <li>• <code>fin</code> = finish (no more data from the user)</li> <li>• <code>psh</code> = push function</li> <li>• <code>rst</code> = reset the connection</li> <li>• <code>syn</code> = synchronize sequence number</li> <li>• <code>urg</code> = urgent field</li> </ul>
<b><i>operator</i></b>	(OPTIONAL) For the TCP and UDP parameters only. Enter one of the following logical operand: <ul style="list-style-type: none"> <li>• <code>eq</code> = equal to</li> <li>• <code>neq</code> = not equal to</li> <li>• <code>gt</code> = greater than</li> <li>• <code>lt</code> = less than</li> <li>• <code>range</code> = inclusive range of ports (you must specify two ports for the port command parameter.)</li> </ul>
<b><i>source port</i></b>	Enter the keywords <code>source-port</code> then the port number to be matched in the ACL rule in the ICAP rule
<b><i>destination-port</i></b>	Enter the keywords <code>destination-port</code> then the port number to be matched in the ACL rule in the ICAP rule.
<b><i>source-port-range</i></b>	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.
<b><i>destination-port-range</i></b>	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.

<b>Defaults</b>	none
<b>Command Modes</b>	REDIRECT-LIST
<b>Supported Modes</b>	Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Added support for <code>track-id</code> on the MXL.
	<b>9.4(0.0)</b>	Added support for removing the Sonet interface on the MXL 10/40GbE Switch IO Module.

# show cam pbr

Displays 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. The range is from 0 to 11.
- port-set *number*** Enter the keywords `port-set` then the port-pipe number. The range is from 0 to 0.
- summary** Enter the keyword `summary` to view only the total number of CAM entries.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Added support for removing the Sonet interface on the MXL 10/40GbE Switch IO Module.
	7.4.1.0	Introduced.

**Usage Information** The `show cam pbr` command displays the PBR CAM content.

## Example

```
Dell#show cam pbr stack-unit 0 po 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  Top Src Dst  SrcIp  DstIp Next-hop  Egress
          Flag  Port  Port
-----
MAC          Port
-----
00000 5 N/A IP    0x0  0  0  22.22.2.22/32  33.33.3.0/24
00:01:e8:8a:fd:76  0/0
00001 5 N/A 145  0x0  0  0  0.0.0.0/0      44.4.4.4/32
00:01:e8:8a:fd:76 V1 100(0/1)
00002 5 N/A TCP  0x0  0  0  55.1.3.0/24    66.6.6.6/32
00:01:e8:8a:fd:76 Po 128
00003 5 N/A UDP  0x0  0  0  55.1.3.0/24    66.6.6.6/32
00:01:e8:8a:fd:76 Po 128
00004 5 N/A IP    0x0  0  0  0.0.0.0/0      0.0.0.0/0
00:01:e8:8a:fd:76 V1 1020 (Po 100)
Dell#
```

- Related Commands**
- [ip redirect-group](#) – applies a redirect group to an interface.
  - [show ip redirect-list](#) – displays the redirect-list configuration.
  - [show cam-usage](#) – displays the CAM usage on ACL, router, or switch.

# 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

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for removing the Sonet interface on the MXL.
7.4.1.0	Introduced.

**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)
seq 10 redirect tunnel 1 track 1 tcp any any,
  Track 1 [up], Next-hop reachable (via Te 1/32)
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)
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 1/9)
, 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 1/10)
, Track 200
[up], Next-hop reachable (via Te 2/11)
```

# PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast (PIM) commands are supported by the Dell Networking Operating System (OS).

This chapter contains the following sections:

- [IPv4 PIM-Sparse Mode Commands](#)
- [IPv6 PIM-Sparse Mode Commands](#)

## Topics:

- [IPv4 PIM-Sparse Mode Commands](#)
- [clear ip pim rp-mapping](#)
- [clear ip pim tib](#)
- [debug ip pim](#)
- [ip pim bsr-border](#)
- [ip pim bsr-candidate](#)
- [ip pim dr-priority](#)
- [ip pim join-filter](#)
- [ip pim ingress-interface-map](#)
- [ip pim neighbor-filter](#)
- [ip pim query-interval](#)
- [ip pim register-filter](#)
- [ip pim rp-address](#)
- [ip pim rp-candidate](#)
- [ip pim sparse-mode](#)
- [ip pim sparse-mode sg-expiry-timer](#)
- [ip pim spt-threshold](#)
- [no ip pim snooping dr-flood](#)
- [show ip pim bsr-router](#)
- [show ip pim interface](#)
- [show ip pim neighbor](#)
- [show ip pim rp](#)
- [show ip pim snooping interface](#)
- [show ip pim snooping neighbor](#)
- [show ip pim snooping tib](#)
- [show ip pim summary](#)
- [show ip pim tib](#)
- [show running-config pim](#)
- [IPv6 PIM-Sparse Mode Commands](#)
- [ipv6 pim bsr-border](#)
- [ipv6 pim bsr-candidate](#)
- [ipv6 pim dr-priority](#)
- [ipv6 pim join-filter](#)
- [ipv6 pim query-interval](#)
- [ipv6 pim neighbor-filter](#)
- [ipv6 pim register-filter](#)
- [ipv6 pim rp-address](#)
- [ipv6 pim rp-candidate](#)
- [ipv6 pim sparse-mode](#)
- [ipv6 pim spt-threshold](#)
- [show ipv6 pim bsr-router](#)
- [show ipv6 pim interface](#)
- [show ipv6 pim neighbor](#)

- `show ipv6 pim rp`
- `show ipv6 pim tib`

## 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** `clear ip pim rp-mapping rp-address`

**Parameters** ***rp-address*** (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### clear ip pim tib

Clear PIM tree information from the PIM database.

**Syntax** `clear ip pim tib [group]`

**Parameters** ***group*** (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 [bsr | events | group | packet [in | out] | register | state | timer [assert | hello | joinprune | register]]`

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all` to disable all the debugging commands.

<b>Parameters</b>	<b>bsr</b>	(OPTIONAL) Enter the keyword <code>bsr</code> to view PIM Candidate RP/BSR activities.
	<b>events</b>	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
	<b>group</b>	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
	<b>packet [in   out]</b>	(OPTIONAL) Enter the keyword <code>packet</code> to view PIM packets. Enter one of the optional parameters: <ul style="list-style-type: none"><li>• <code>in</code>: to view incoming packets</li><li>• <code>out</code>: to view outgoing packets</li></ul>
	<b>register</b>	(OPTIONAL) Enter the keyword <code>register</code> to view PIM register address in dotted decimal format (A.B.C.D).
	<b>state</b>	(OPTIONAL) Enter the keyword <code>state</code> to view PIM state changes.
	<b>timer [assert   hello   joinprune   register]</b>	(OPTIONAL) Enter the keyword <code>timer</code> to view PIM timers. Enter one of the optional parameters: <ul style="list-style-type: none"><li>• <code>assert</code>: to view the assertion timer</li><li>• <code>hello</code>: to view the PIM neighbor keepalive timer</li><li>• <code>joinprune</code>: to view the expiry timer (join/prune timer)</li><li>• <code>register</code>: to view the register suppression timer</li></ul>

**Defaults** Disabled.

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

**Syntax** `ip pim bsr-border`  
To return to the default value, use the `no ip pim bsr-border` command.

**Defaults** Disabled.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time-out. To clean the candidate RP advertisements, use the `clear ip pim rp-mapping` command.



# ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

**Syntax** `ip pim bsr-candidate interface [hash-mask-length] [priority]`

To return to the default value, use the `no ip pim bsr-candidate` command.

**Parameters**

<b>interface</b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>• For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>
------------------	---

**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

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ip pim dr-priority

Change the designated router (DR) priority for the interface.

**Syntax** `ip pim dr-priority priority-value`

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

**Parameters**

<b>priority-value</b>	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

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `ip pim join-filter ext-access-list {in | out}`  
To remove the access list, use the `no ip pim join-filter ext-access-list {in | out}` command.

**Parameters**

- ext-access-list** Enter the name of an extended access list.
- in** Enter this keyword to apply the access list to inbound traffic.
- out** Enter this keyword to apply the access list to outbound traffic.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

**Usage Information** When you configure a join filter, it is applicable for both ingress and egress flows. There is no option to specify in or out parameters while configuring a join filter.

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell(conf)# ip access-list extended iptv-channels
Dell(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
Dell(config-ext-nacl)# permit ip any 232.1.1.0/24
Dell(config-ext-nacl)# permit ip 100.1.1.0/16 any
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels
```

**Related Commands** [ip access-list extended](#) — configure an access list based on IP addresses or protocols.

# ip pim ingress-interface-map

When the Dell Networking system is the RP, statically map potential incoming interfaces to (\*,G) entries to create a lossless multicast forwarding environment.

**Syntax** `ip pim ingress-interface-map std-access-list`

**Parameters**

- std-access-list** Enter the name of a standard access list.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell(conf)# ip access-list standard map1
Dell(config-std-nacl)# permit 224.0.0.1/24
```

```
Dell(config-std-nacl)#exit
Dell(conf)#int te 0/1
Dell(config-if-te-0/1)# ip pim ingress-interface-map map1
```

## ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

**Syntax** `ip pim neighbor-filter {access-list}`  
To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

**Parameters** **access-list** Enter the name of a standard access list. Maximum 16 characters.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 register-filter access-list`  
To return to the default, use the `no ip pim register-filter access-list` command.

<b>Parameters</b>	<b><i>access-list</i></b>	Enter the name of an extended access list. Maximum 16 characters.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip pim rp-address address {group-address group-address mask} override</code>	
	To remove an RP address, use the <code>no ip pim rp-address address {group-address group-address mask} override</code> command.	
<b>Parameters</b>	<b><i>address</i></b>	Enter the RP address in dotted decimal format (A.B.C.D).
	<b><i>group-address group-address mask</i></b>	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.
	<b><i>override</i></b>	Enter the keyword <code>override</code> to override the BSR updates with static RP. The <code>override</code> takes effect immediately during enable/disable.
	 <b>NOTE:</b> This option is applicable to multicast group range.	
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip pim rp-candidate {interface [priority] [acl-name]}</code>	
	To return to the default value, use the <code>no ip pim rp-candidate {interface [priority]}</code> command.	
<b>Parameters</b>	<b><i>interface</i></b>	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 information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**priority**

(OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is **192**.

**acl-name**

(OPTIONAL) Enter the name of an ACL to configure a PIM router to act as an RP for a specific set of multicast group addresses that are defined in the ACL.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.11.0.0**

Introduced the `acl-name` keyword.

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full—Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.2(0.0)**

Introduced on the MXL 10/40GbE Switch IO Module.

**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, or for a specific set of (S,G) pairs an access list defines.

**Syntax**

`ip pim sparse-mode sg-expiry-timer seconds [access-list name]`

To disable configured timers and return to default mode, use the `no ip pim sparse-mode sg-expiry-timer` command.

<b>Parameters</b>	<b>seconds</b>	Enter the number of seconds the S, G entries are retained. The range is from 211 to 86400.
	<b>access-list name</b>	(OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries.
<b>Defaults</b>	Disabled. The default expiry timer (with no times configured) is 210 sec.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.	

## ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

<b>Syntax</b>	<code>ip pim spt-threshold value   infinity</code>	
	To return to the default value, use the <code>no ip pim spt-threshold</code> command.	
<b>Parameters</b>	<b>value</b>	(OPTIONAL) Enter the traffic value in kilobits per second. The default is <b>10 packets per second</b> . A value of zero (0) causes a switchover on the first packet.
	<b>infinity</b>	(OPTIONAL) Enter the keyword <code>infinity</code> to never switch to the source-tree.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	This command is applicable to last hop routers on the shared tree towards the rendezvous point (RP).	

## no ip pim snooping dr-flood

Disable the flooding of multicast packets to the PIM designated router.

<b>Syntax</b>	<code>no ip pim snooping dr-flood</code>	
	To re-enable the flooding of multicast packets to the PIM designated router, use the <code>ip pim snooping dr-flood</code> command.	
<b>Defaults</b>	Enabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switch	

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>By default, when you enable PIM-SM snooping, a switch floods all multicast traffic to the PIM designated router (DR), including unnecessary multicast packets. To minimize the traffic sent over the network to the designated router, you can disable <code>designated-router flooding</code>.</p> <p>When <code>designated-router flooding</code> is disabled, PIM-SM snooping only forwards the multicast traffic, which belongs to a multicast group for which the switch receives a join request, on the port connected towards the designated router.</p> <p>If the PIM DR flood is not disabled (default setting):</p> <ul style="list-style-type: none"> <li>• Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.</li> <li>• Multicast traffic for an unknown group is sent on the port towards the PIM DR. When DR flooding is disabled, multicast traffic for an unknown group is dropped.</li> </ul>						
<b>Related Commands</b>	<a href="#">ip pim sparse-mode</a> — enables PIM-SM snooping.						

## show ip pim bsr-router

View information on the Bootstrap router.

**Syntax** `show ip pim bsr-router`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

### Example

```
E600-7-rpm0#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  Uptime: 16:59:06, 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.

**Syntax** `show ip pim interface`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip pim interface` command shown in the following example.

Field	Description
<b>Address</b>	Lists the IP addresses of the interfaces participating in PIM.
<b>Interface</b>	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
<b>Ver/Mode</b>	Displays the PIM version number and mode for each interface participating in PIM: <ul style="list-style-type: none"> <li>v2 = PIM version 2</li> <li>S = PIM Sparse mode</li> </ul>
<b>Nbr Count</b>	Displays the number of PIM neighbors discovered over this interface.
<b>Query Intvl</b>	Displays the query interval for Router Query messages on that interface (configured with <code>ip pim query-interval</code> command).
<b>DR Prio</b>	Displays the Designated Router priority value configured on the interface (use the <code>ip pim dr-priority</code> command).
<b>DR</b>	Displays the IP address of the Designated Router for that interface.

**Example**

```
E600-7-RPM0#show ip pim interface
Address          Interface Ver/  Nbr  Query DR   DR
                  Mode Count Intvl Prio
172.21.200.254  te 0/5   v2/S 0    30 1 172.21.200.254
172.60.1.2      te 0/1   v2/S 0    30 1 172.60.1.2
192.3.1.1       te 1/8   v2/S 1    30 1 192.3.1.1
192.4.1.1       te 1/8   v2/S 0    30 1 192.4.1.1
172.21.110.1    te 1/6   v2/S 0    30 1 172.21.110.1
172.21.203.1    te 1/7   v2/S 0    30 1 172.21.203.1
```

## show ip pim neighbor

View PIM neighbors.

**Syntax** `show ip pim neighbor`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip pim neighbor` command shown in the following example.

Field	Description
<b>Neighbor address</b>	Displays the IP address of the PIM neighbor.
<b>Interface</b>	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.



Field	Description
<b>Uptime/expires</b>	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).
<b>Ver</b>	Displays the PIM version number. <ul style="list-style-type: none"> <li>v2 = PIM version 2</li> </ul>
<b>DR prio/Mode</b>	Displays the Designated Router priority and the mode. <ul style="list-style-type: none"> <li>1 = default Designated Router priority (use the <code>ip pim dr-priority</code> command)</li> <li>DR = Designated Router</li> <li>S = Sparse mode</li> </ul>

### Example

```
Dell#show ip pim neighbor
Neighbor   Interface  Uptime/Expires   Ver   DR
Address
127.87.3.4 te 1/7      09:44:58/00:01:24 v2    1 / S
Dell#
```

## show ip pim rp

View all multicast groups-to-RP mappings.

**Syntax** `show ip pim rp [mapping | group-address]`

**Parameters**

- mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
- group-address** (OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#sh 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#sh ip pim rp mapping
Group(s): 224.0.0.0/4
RP: 165.87.20.4, v2
Info source: 165.87.20.5, via bootstrap, priority 0
Uptime: 00:03:11, expires: 00:02:46
RP: 165.87.20.3, v2
Info source: 165.87.20.5, via bootstrap, priority 0
```

```
Uptime: 00:03:11, expires: 00:03:03
```

```
Dell#
```

### Example (Address)

```
Dell#sh ip pim rp 229.1.2.1
Group          RP
229.1.2.1      165.87.20.4

Dell#
```

## show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

**Syntax** `show ip pim snooping interface [vlan vlan-id]`

**Parameters** **vlan *vlan-id*** (OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN IDs range is from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

The following describes the `show ip pim snooping interface` commands shown in the following example.

Field	Description
<b>Interface</b>	Displays the VLAN interfaces with PIM-SM snooping enabled.
<b>Ver/Mode</b>	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: <ul style="list-style-type: none"><li>• v2 = PIM version 2</li><li>• S = PIM Sparse mode</li></ul>
<b>Nbr Count</b>	Displays the number of neighbors learned through PIM-SM snooping on the interface.
<b>DR Prio</b>	Displays the Designated Router priority value configured on the interface ( <code>ip pim dr-priority</code> command).
<b>DR</b>	Displays the IP address of the Designated Router for that interface.

### Example (#2)

```
Dell#show ip pim snooping interface
Interface Ver Nbr   DR   DR
          Count Prio
Vlan 2    v2  3    1    165.87.32.2
```

## show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

**Syntax** `show ip pim snooping neighbor [vlan vlan-id]`

**Parameters**      **vlan *vlan-id***      (OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
---------	-------------

<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**      The following describes the `show ip pim snooping neighbor` commands shown in the following example.

Field	Description
<b>Neighbor address</b>	Displays the IP address of the neighbor learned through PIM-SM snooping.
<b>Interface</b>	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
<b>Uptime/expires</b>	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).
<b>Ver</b>	Displays the PIM version number: <ul style="list-style-type: none"> <li>• v2 = PIM version 2</li> </ul>
<b>DR prio/Mode</b>	Displays the Designated Router priority and the mode: <ul style="list-style-type: none"> <li>• 1 = default Designated Router priority (use the <code>ip pim dr-priority</code> command)</li> <li>• DR = Designated Router</li> <li>• S = Sparse mode</li> </ul>

### Example

```
Dell#show ip pim snooping neighbor

Neighbor      Interface          Uptime/Expires    Ver  DR Prio
Address
165.87.32.2   V1 2 [tei 4/8 ]    00:04:03/00:01:42 v2   1
165.87.32.10 V1 2 [te 4/8 ]     00:00:46/00:01:29 v2   0
165.87.32.12 V1 2 [te 4/8 ]     00:00:51/00:01:24 v2   0
```

## show ip pim snooping tib

Display information from the tree information base (TIB) PIM-SM snooping discovered about multicast group members and states.

**Syntax**      `show ip pim snooping tib [vlan vlan-id] [group-address [source-address]]`

**Parameters**

**vlan *vlan-id***      (OPTIONAL) Enter a VLAN ID to display TIB information PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

***group-address***      (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast group.

***source-address***      (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D) to display TIB information PIM-SM snooping discovered for a specified multicast source.

**Command Modes**      • EXEC

- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following describes the `show ip pim snooping tib` commands shown in the following example.

Field	Description
<b>(S, G)</b>	Displays the entry in the PIM multicast snooping database.
<b>uptime</b>	Displays the amount of time the entry has been in the PIM multicast route table.
<b>expires</b>	Displays the amount of time until the entry expires and is removed from the database.
<b>RP</b>	Displays the IP address of the RP/source for this entry.
<b>flags</b>	List the flags to define the entries: <ul style="list-style-type: none"> <li>• S = PIM Sparse Mode</li> <li>• C = directly connected</li> <li>• L = local to the multicast group</li> <li>• P = route was pruned</li> <li>• R = the forwarding entry is pointing toward the RP</li> <li>• F = Dell Networking OS is registering this entry for a multicast source</li> <li>• T = packets were received via Shortest Tree Path</li> <li>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</li> <li>• K=acknowledge pending state</li> </ul>
<b>Incoming interface</b>	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
<b>RPF neighbor</b>	Displays the next hop from this interface towards the RP/source.
<b>Outgoing interface list:</b>	Lists the interfaces that meet one of the following criteria: <ul style="list-style-type: none"> <li>• a directly connect member of the Group</li> <li>• statically configured member of the Group</li> <li>• received a (*,G) Join message</li> </ul>

**Example**

```
Dell#show ip pim snooping tib

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
      SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port

(*, 225.1.2.1), uptime 00:00:01, expires 00:02:59, RP 165.87.70.1,
flags: J
  Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
  Outgoing interface list:
    TenGigabitEthernet 4/5 RPF 165.87.32.2 00:00:01/00:02:59
    TenGigabitEthernet 4/6 Upstream Port -/-

Dell#show ip pim snooping tib vlan 2 225.1.2.1 165.87.1.7

PIM Multicast Snooping Table
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
      SGR-P - (S,G,R) Prune
Timers: Uptime/Expires
* : Inherited port
```

```
(165.87.1.7, 225.1.2.1), uptime 00:00:08, expires 00:02:52, flags: j
Incoming interface: Vlan 2, RPF neighbor 0.0.0.0
Outgoing interface list:
  TenGigabitEthernet 4/7 Upstream Port    -/-
  TenGigabitEthernet 4/6 DR Port          -/-
  TenGigabitEthernet 4/8 RPF 165.87.32.10 00:00:08/00:02:52
```

## show ip pim summary

View information about PIM-SM operation.

**Syntax** `show ip pim summary`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

Memory usage:
  TIB : 3768 bytes
  Nexthop cache : 0 bytes
```

```
Interface table : 992 bytes
Neighbor table : 528 bytes
RP Mapping      : 0 bytes
```

## show ip pim tib

View the PIM tree information base (TIB).

**Syntax** `show ip pim tib [group-address [source-address]]`

**Parameters**

- group-address** (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
- source-address** (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip pim tib` command shown in the following example.

Field	Description
<b>(S, G)</b>	Displays the entry in the multicast PIM database.
<b>uptime</b>	Displays the amount of time the entry has been in the PIM route table.
<b>expires</b>	Displays the amount of time until the entry expires and is removed from the database.
<b>RP</b>	Displays the IP address of the RP/source for this entry.
<b>flags</b>	List the flags to define the entries: <ul style="list-style-type: none"> <li>• D = PIM Dense Mode</li> <li>• S = PIM Sparse Mode</li> <li>• C = directly connected</li> <li>• L = local to the multicast group</li> <li>• P = route was pruned</li> <li>• R = the forwarding entry is pointing toward the RP</li> <li>• F = Dell Networking OS is registering this entry for a multicast source</li> <li>• T = packets were received via Shortest Tree Path</li> <li>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</li> <li>• K = acknowledge pending state</li> </ul>
<b>Incoming interface</b>	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
<b>RPF neighbor</b>	Displays the next hop from this interface towards the RP/source.
<b>Outgoing interface list:</b>	Lists the interfaces that meet one of the following criteria: <ul style="list-style-type: none"> <li>• a directly connect member of the Group</li> <li>• statically configured member of the Group</li> <li>• received a (*,G) Join message</li> </ul>

### Example

```
Dell#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

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP 10.211.2.1, flags:
SCJ
  Incoming interface: TenGigabitEthernet 0/2, RPF neighbor 10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 0/8

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags:
SCJ
  Incoming interface: TenGigabitEthernet 1/2, RPF neighbor 10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 0/8

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags:
SCJ
  Incoming interface: TenGigabitEthernet 1/2, RPF neighbor 10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 0/8

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags:
SCJ
  Incoming interface: TenGigabitEthernet 1/2, RPF neighbor 10.211.1.2
  Outgoing interface list:
    TenGigabitEthernet 0/8

```

## show running-config pim

Display the current configuration of PIM-SM snooping.

**Syntax** `show running-config pim`

**Command Modes** EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```

Dell#show running-config pim
!
ip pim snooping enable

```

**Related Commands** [ip pim sparse-mode](#) — enables PIM-SM snooping.

## IPv6 PIM-Sparse Mode Commands

The following describes the IPv6 PIM-sparse mode (PIM-SM) commands.

# ipv6 pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

**Syntax** `ipv6 pim bsr-border`

**Defaults** Disabled.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is applied to the subsequent PIM-BSR messages. Existing BSR advertisements are cleaned up by time-out.

# ipv6 pim bsr-candidate

Configure the router as a bootstrap (BSR) candidate.

**Syntax** `ipv6 pim bsr-candidate interface [hash-mask-length] [priority]`  
To disable the bootstrap candidate, use the `no ipv6 pim bsr-candidate` command.

Parameters		
<b>interface</b>	Enter the following keywords and slot/port or number information:	
	<ul style="list-style-type: none"><li>For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li><li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number.</li><li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>	
<b>hash-mask-length</b>	(OPTIONAL) Enter the hash mask length for RP selection. The range is from 0 to 128. The default is <b>126</b> .	
<b>priority</b>	(OPTIONAL) Enter the priority value for Bootstrap election process. The range is from 0 to 255. The default is <b>0</b> .	

**Defaults** Refer to Parameters.

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

**Syntax** `ipv6 pim dr-priority priority-value`  
To remove the DR priority value assigned, use the `no ipv6 pim dr-priority` command.



<b>Parameters</b>	<b><i>priority-value</i></b>	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is <b>1</b> .
<b>Defaults</b>	<b>1</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.	

## ipv6 pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

**Syntax** `ipv6 pim join-filter access-list`

<b>Parameters</b>	<b><i>access-list</i></b>	Enter the name of an extended access list.
	<b>in</b>	Enter the keyword <code>in</code> to apply the access list to inbound traffic.
	<b>out</b>	Enter the keyword <code>out</code> to apply the access list to outbound traffic.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf)#ipv6 access-list JOIN-FIL_ACL
Dell(conf-ipv6-acl)#permit ipv6 165:87:34::0/112 ff0e::225:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 any ff0e::230:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 165:87:32::0/112 any
Dell(conf-ipv6-acl)#exit
Dell(conf)#interface tengigabitethernet 0/84
Dell(conf-if-te-0/84)#ipv6 pim join-filter JOIN-FIL_ACL in
Dell(conf-if-te-0/84)#ipv6 pim join-filter JOIN-FIL_ACL out
```

## ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

**Syntax** `ipv6 pim query-interval seconds`

To return to the default value, use the `no ipv6 pim query-interval seconds` command.

<b>Parameters</b>	<b><i>seconds</i></b>	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is <b>30 seconds</b> .
-------------------	-----------------------	---

<b>Defaults</b>	<b>30 seconds</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full—Switich	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 pim neighbor-filter

Prevent the system from forming a PIM adjacency with a neighboring system.

<b>Syntax</b>	<code>ipv6 pim neighbor-filter {access-list}</code>	
<b>Parameters</b>	<b><i>access-list</i></b>	Enter the name of a standard access list. Maximum 16 characters.
<b>Defaults</b>	none	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switich	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	Do not enter this command before creating the access-list.	

## ipv6 pim register-filter

Configure the source DR so that it does not send register packets to the RP for the specified sources and groups.

<b>Syntax</b>	<code>ipv6 pim register-filter access-list</code>	
<b>Parameters</b>	<b><i>access-list</i></b>	Enter the name of the extended ACL that contains the sources and groups to filter.
<b>Defaults</b>	none	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full—Switich	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf)#ipv6 pim register-filter REG-FIL_ACL
Dell(conf)#ipv6 access-list REG-FIL_ACL
Dell(conf-ipv6-acl)#deny ipv6 165:87:34::10/128 ff0e::225:1:2:0/112
Dell(conf-ipv6-acl)#permit ipv6 any any
Dell(conf-ipv6-acl)#exit
```

# ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. First-hop routers use this address to send register packets on behalf of the source multicast host.

**Syntax** `ipv6 pim rp-address address group-address group-address mask override`  
To remove an RP address, use the `no ipv6 pim re-address address group-address mask override` command.

**Parameters**

- address** Enter the IPv6 RP address in the x:x:x::x format.  
**NOTE:** The :: notation specifies successive hexadecimal fields of zero.
- group-address** Enter the keywords `group-address` then the group address in the x:x:x::x format and then the mask in /nn format to assign that group address to the RP.  
**NOTE:** The :: notation specifies successive hexadecimal fields of zero.
- group-address**
- mask**
- override** Enter the keyword `override` to override the BSR updates with static RP. The `override` takes effect immediately during `enable/disable`.  
**NOTE:** This option is applicable to multicast group range.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses.

Without the `override` option, the BSR-advertised RPs updates take precedence over the statically configured RPs.

# ipv6 pim rp-candidate

Specify an interface as an RP candidate.

**Syntax** `ipv6 pim rp-candidate interface [priority-value]`

**Parameters**

- interface** Enter the following keywords and slot/port or number information:
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
- priority-value** (OPTIONAL) Enter a number as the priority of this RP Candidate, which is included in the Candidate-RP-Advertisements. The range is 0 (highest) to 255 (lowest).

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode on the interface.

**Syntax** `ipv6 pim sparse-mode`  
To disable IPv6 PIM sparse mode, use the `no ipv6 pim sparse-mode` command.

**Defaults** Disabled.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Enable the interface (use the `no shutdown` command) and not have the `switchport` command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.

## ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

**Syntax** `ipv6 pim spt-threshold {kbps | infinity}`  
To return to the default value, use the `no ipv6 pim spt-threshold` command.

**Parameters**

<b><i>kbps</i></b>	Enter a traffic rate in kilobytes per second. The range is from 0 to 4294967 kbps. The default is <b>10 kbps</b> .
<b><i>infinity</i></b>	Enter the keyword <code>infinity</code> to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

**Defaults** **10 kbps**

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

## show ipv6 pim bsr-router

View information on the Bootstrap router (v2).

**Syntax** `show ipv6 pim bsr-router`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 14::2
  Uptime:      00:02:54, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:06

This system is a candidate BSR
  Candidate BSR address: 14::2, priority: 0, hash mask length: 126
Dell
```

## show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

**Syntax** `show ipv6 pim interface`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#show ipv6 pim interface
Interface Ver/ Nbr  Query DR
          Mode Count Intvl Prio

Te 0/3   v2/S 1    30    1
  Address : fe80::201:e8ff:fe02:140f
  DR      : this router

Te 0/1   v2/S 0    30    1
  Address : fe80::201:e8ff:fe02:1417
  DR      : this router
Dell#
```

# show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

**Syntax** `show ipv6 pim neighbor [detail]`

**Parameters** **detail** (OPTIONAL) Enter the keyword `detail` to displayed PIM neighbor detailed information.

**Supported Modes** Full—Switch

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell#show ipv6 pim neighbor detail
Neighbor Interface Uptime/Expires Ver DR
Address                               Prio/Mode
fe80::201:e8ff:fe00:6265 Te 0/3 00:07:39/00:01:42 v2 1 / S
165:87:50::6
Dell#
```

# show ipv6 pim rp

View all multicast groups-to-RP mappings.

**Syntax** `show ipv6 pim rp [mapping | group-address]`

**Parameters** **mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.

**group-address** (OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dellshow ipv6 pim rp
Group RP
ff0e::225:1:2:1 14::1
ff0e::225:1:2:2 14::1
ff0e::226:1:2:1 14::1
ff0e::226:1:2:2 14::1
Dell
```

**Example (Mapping)**

```
Dellshow ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
RP: 14::1, v2
```

```

Info source: 14::1, via bootstrap, priority 192
  Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
Dell

```


## show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base — tib).


**Syntax** `show ipv6 pim tib [group-address [source-address]]`

**Parameters**

**group-address** (OPTIONAL) Enter the multicast group address in the x:x:x:x format to view RP mappings for a specific group.

 **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

**source-address** (OPTIONAL) Enter the source address in the x:x:x:x format.

 **NOTE:** The :: notation specifies successive hexadecimal fields of zero.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
---------	-------------

9.9(0.0)	Introduced on the FN IOM.
----------	---------------------------

9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.
----------	--

### Example

```

Dell#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires 00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 0/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/1

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 0/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/1

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 0/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/1

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires 00:00:00, flags: CJ
  RPF neighbor: TenGigabitEthernet 0/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/1
Dell#

```

## 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 only. Port-channel interfaces and virtual local area networks (VLANs), are not supported.
- The monitoring (destination, “MG”) and monitored (source, “MD”) ports must be on the same switch.
- The monitored (source) interface must be a server-facing interface in the format slot/port, where valid slot number is 0 and server-facing port numbers are from 1 to 8. The monitoring interface must be an uplink port in the chassis.
- Dell Networking OS permits a limited set of commands for monitoring ports. To display these commands, use the ? command.
- A monitoring port may not be a member of a VLAN.
- There may only be one destination port in a monitoring session.
- A source port (MD) can only be monitored by one destination port (MG). If you try to assign a monitored port to more than one monitoring port, the following error is displayed as shown in example.

#### Example

```
Dell(conf)#mon ses 1
Dell(conf-mon-sess-1)#source tengig 0/1 destination tengig 0/6 direction
both
Dell(conf-mon-sess-1)#do show mon ses
SessionID Source      Destination  Direction  Mode  Type
-----
1      TenGig 0/1  TenGig 0/6  both           interface
Port-based
Dell(conf-mon-sess-1)#mon ses 2
Dell(conf-mon-sess-2)#source tengig 0/1 destination tengig 0/7 direction
both
% Error: MD port is already being monitored.
```

**NOTE:** There is no limit to the number of monitoring sessions per system, provided that there are only four destination ports per port-pipe. If each monitoring session has a unique destination port, the maximum number of session is four per port-pipe.

#### Topics:

- [description](#)
- [erpm](#)
- [flow-based enable](#)
- [rate-limit](#)
- [monitor session](#)
- [show config](#)
- [show monitor session](#)
- [show running-config monitor session](#)
- [source \(port monitoring\)](#)

### 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**      MONITOR SESSION (conf-mon-sess-session-ID)

**Supported Modes**      All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## erpm

Configure the source and destination IP address for ERPM traffic.

**Syntax**      `erpm source-ip ip-address dest-ip ip-address [gre-protocol value]`  
To remove the configuration, use the `no erpm source-ip IP-address dest-ip IP-address [gre-protocol value]` command.

**Parameters**

<b>source-ip ip-address</b>	Enter the keywords <code>source-ip</code> then the source IP address in dotted decimal format.
<b>destination-ip ip-address</b>	Enter the keywords <code>dest-ip</code> then the destination IP address in dotted decimal format.
<b>gre-protocol value</b>	(OPTIONAL) Enter the keywords <code>gre-protocol</code> then the protocol type value for ERPM type monitor session. The range is from 1 to 65535.

**Command Modes**      MONITOR SESSION (conf-mon- sess-session-ID)

**Example**

```
Dell(conf-mon-sess-10)#erpm source-ip 10.10.10.1 dest-ip 5.1.1.2 gre-protocol 1111
```

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

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

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced GRE protocol support.

**Related Commands**

- [monitor session](#) — creates a session for monitoring traffic with port monitoring.
- [show monitor session](#) — displays information about monitor configurations.

## flow-based enable

Enable flow-based monitoring.

**Syntax**      `flow-based enable`  
To disable flow-based monitoring, use the `no flow-based enable` command.

**Defaults**      Disabled, that is flow-based monitoring is not applied.

**Command Modes** MONITOR SESSION (*conf-mon-sess-session-ID*)

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Added support for the RPM/ERPM.
9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.
8.1.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced on the E-Series.

**Usage Information**

To monitor traffic with particular flows the interface, appropriate ACLs has be applied in ingress direction. Flow- based is not supported in the tx direction. Even though we can configure it in both the direction, only rx will work.

The flow- based enable command has to be applied as a `monitor session` with some configuration which is already present in it, other wise flow- based will not take effect.

**Related Commands**

[monitor session](#) – enables a monitoring 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

**Supported Modes** Full—Switch

**Command History**

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

[monitor session](#) — enables a monitoring session.

[show monitor session](#) — displays the monitor session.

## monitor session

Create a session for monitoring traffic with port monitoring.

**Syntax**

```
monitor session session-ID (type { rpm | erpm }) [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.

<b>Parameters</b>	<b>session-ID</b>	Enter a session identification number. The range is from 0 to 65535.
	<b>type rpm / erpm</b>	Specifies one of the following type: <ul style="list-style-type: none"> <li>rpm: to create remote port monitoring session.</li> <li>erpm: to create encapsulated remote port monitoring session.</li> <li>If no option is specified, by default SPAN will be created.</li> </ul>
		<b>NOTE:</b> The rpm and erpm options are supported only in Full-Switch mode.
	<b>drop</b>	Monitors only the dropped packets in the Ingress.

<b>Defaults</b>	none
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Added the drop parameter.
	<b>9.4(0.0)</b>	Added support for rpm / erpm.
	<b>8.3.16.1</b>	Introduced on the M I/O Aggregator.

**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(conf)# monitor session 60
Dell(conf-mon-sess-60)
```

**Related Command**

[show monitor session](#) — displays the monitor session.

[show running-config monitor session](#) — displays the running configuration of a monitor session.

## show config

Display the current monitor session configuration.

<b>Syntax</b>	show config	
<b>Defaults</b>	none	
<b>Command Modes</b>	MONITOR SESSION (conf-mon-sess-session-ID)	
<b>Supported Modes</b>	All Modes	
Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Example**

```
Dell(conf-mon-sess-5)#show config
!
monitor session 5
source TenGigabitEthernet 0/4 destination TenGigabitEthernet 0/7
direction rx
Dell(conf-mon-sess-5)#
```

# show monitor session

Display the monitor information of a particular session or all sessions.

**Syntax** `show monitor session {session-ID}`  
To display monitoring information for all sessions, use the `show monitor session` command.

**Parameters** *session-ID* (OPTIONAL) Enter a session identification number. The range is from 0 to 65535.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.

## Example

```
Dell#show monitor session 5
SessionID Source Destination Direction Mode Type
-----
5 Te 0/4 Te 0/3 rx interface Port-based
Dell#
```

**Related Commands** [monitor session](#) — creates a session for monitoring.

# show running-config monitor session

Displays 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 is from 0 to 65535.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**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 run monitor session
!
monitor session 5
source TenGigabitEthernet 0/4 destination TenGigabitEthernet 0/5
direction rx
!
```

```

monitor session 20
source TenGigabitEthernet 0/3 destination TenGigabitEthernet 0/2
direction both
Dell#
Dell#show run monitor session 20
!
monitor session 20
source TenGigabitEthernet 0/3 destination TenGigabitEthernet 0/2
direction both
Dell#

```

**Related Commands**

- [monitor session](#) — creates a session for monitoring.
- [show monitor session](#) — displays a monitor session.

## source (port monitoring)

Configure a port monitor source.

**Syntax** `source interface destination interface direction {rx | tx | both}`

To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

**Parameters**

- interface*** Enter the one of the following keywords and slot/port information:
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- destination*** Enter the keyword `destination` to indicate the interface destination.
- direction {rx | tx | both}*** Enter the keyword `direction` followed by 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*)

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Example**

```

Dell(conf-mon-sess-11)#source tengig 0/1 destination tengig 0/8 direction
rx
Dell(conf-mon-sess-11)#

```

**Usage Information** The monitored (source) interface must be a server-facing interface in the format slot/port, where valid slot number is 0 and server-facing port numbers are from 1 to 8.

## Private VLAN (PVLAN)

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 the Dell Networking OS version 7.8.1.0 at later to provide PVLAN data:

- [show arp](#)
- [show vlan](#)

### Private VLAN Concepts

#### Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

#### Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

#### Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice versa.

#### Port Types:

- *Community port*: A community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- *Isolated port*: An isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- *Promiscuous port*: A promiscuous port is a port that is allowed to communicate with any other port type.
- *Trunk port*: A trunk port carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - A trunk port in Tagged mode carries primary or secondary VLAN traffic. The tag on the packet helps identify the VLAN to which the packet belongs.
  - A trunk port can also belong to a regular VLAN (non-private VLAN).

#### Topics:

- [ip local-proxy-arp](#)
- [private-vlan mapping secondary-vlan](#)
- [private-vlan mode](#)
- [show interfaces private-vlan](#)
- [show vlan private-vlan](#)
- [show vlan private-vlan mapping](#)
- [switchport mode private-vlan](#)

# ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

**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

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.
- [private-vlan mapping secondary-vlan](#) — maps secondary VLANs to the selected primary VLAN.
- [show arp](#) — displays the ARP table.
- [show interfaces private-vlan](#) — displays the type and status of the PVLAN interfaces.
- [show vlan private-vlan](#) — displays the PVLANS and/or interfaces that are part of a PVLAN.
- [switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

# private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

**Syntax** `[no] private-vlan mapping secondary-vlan vlan-list`

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` command syntax.

**Parameters** *vlan-list* Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.

**Defaults** none

**Command Modes** INTERFACE VLAN

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.

- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.

### Related Commands

[private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.

[show interfaces private-vlan](#) — displays the type and status of the PVLAN interfaces.

[show vlan private-vlan](#) — displays the PVLANS and/or interfaces that are part of a PVLAN.

[show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.

[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.

**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**

<b>community</b>	Enter the keyword <code>community</code> to set the VLAN as a community VLAN.
<b>isolated</b>	Enter the keyword <code>isolated</code> to configure the VLAN as an isolated VLAN.
<b>primary</b>	Enter the keyword <code>primary</code> to configure the VLAN as a primary VLAN.

**Defaults** none

**Command Modes** INTERFACE VLAN

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

[show interfaces private-vlan](#) — displays the type and status of the PVLAN interfaces.

[show vlan private-vlan](#) — displays the PVLANS and/or interfaces that are part of a PVLAN.

[show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.

[switchport mode private-vlan](#) — sets PVLAN mode of the selected port.



# show interfaces private-vlan

Display type and status of PVLAN interfaces.

- Syntax** `show interfaces private-vlan [interface interface]`
- Parameters**
  - interface** (OPTIONAL) Enter the keyword *interface* then the ID of the specific interface for which to display PVLAN status.
  - interface***
- Defaults** none
- Command Modes**
  - EXEC
  - EXEC Privilege
- Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

The following describes the `show interfaces private-vlan` command shown in the following examples.

Field	Description
<b>Interface</b>	Displays the type of interface and associated slot and port number.
<b>Vlan</b>	Displays the VLAN ID of the designated interface.
<b>PVLAN-Type</b>	Displays the type of VLAN in which the designated interface resides.
<b>Interface Type</b>	Displays the PVLAN port type of the designated interface.
<b>Status</b>	States whether the interface is operationally up or down.

## Example (All)

```
Dell# show interfaces private-vlan
Interface Vlan PVLAN-Type Interface Type Status
-----
Gi 2/1    10    Primary    Promiscuous    Up
Gi 2/2    100   Isolated   Host           Down
Gi 2/3    10    Primary    Trunk          Up
Gi 2/4    101   Community  Host           Up
```

## Example (Specific)

```
Dell# show interfaces private-vlan Gi 2/2
Interface Vlan PVLAN-Type Interface Type Status
-----
Gi 2/2    100   Isolated   Host           Up
```

## Related Commands

- [private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.
- [show vlan private-vlan](#) — displays the PVLANS and/or interfaces that are part of a PVLAN.
- [show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.
- [switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

# show vlan private-vlan

Display PVLANS and/or interfaces that are part of a PVLAN.

**Syntax** `show vlan private-vlan [community | interface | isolated | primary | primary_vlan | interface interface]`

<b>Parameters</b>	<b>community</b>	(OPTIONAL) Enter the keyword <code>community</code> to display VLANs configured as community VLANs, along with their interfaces.
	<b>interface</b>	(OPTIONAL) Enter the keyword <code>interface</code> to display VLANs configured as community VLANs, along with their interfaces.
	<b>isolated</b>	(OPTIONAL) Enter the keyword <code>isolated</code> to display VLANs configured as isolated VLANs, along with their interfaces.
	<b>primary</b>	(OPTIONAL) Enter the keyword <code>primary</code> to display VLANs configured as primary VLANs, along with their interfaces.
	<b>primary_vlan</b>	(OPTIONAL) Enter a private VLAN ID or secondary VLAN ID to display interface details about the designated PVLAN.
	<b>interface interface</b>	(OPTIONAL) Enter the keyword <code>interface</code> and an interface ID to display the PVLAN configuration of the designated interface.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full—Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANS and their member VLANs and interfaces. The other types of output show details about PVLAN subsets.

The following describes the `show private-vlan` command shown in the Examples below.

Field	Description
<b>Primary</b>	Displays the VLAN ID of the designated or associated primary VLAN(s).
<b>Secondary</b>	Displays the VLAN ID of the designated or associated secondary VLAN(s).
<b>Type</b>	Displays the type of VLAN in which the listed interfaces reside.
<b>Active</b>	States whether the interface is operationally up or down.
<b>Ports</b>	Displays the interface IDs in the listed VLAN.

## Example (All)

```
Dell# show vlan private-vlan
Primary Secondary Type Active Ports
-----
10          100      primary   Yes   Gi 2/1,3
            101      isolated  Yes   Gi 2/2
            101      community Yes   Gi 2/10
20          200      primary   Yes   Po 10, 12-13
            200      primary   Yes   Gi 3/1
            200      isolated  Yes   Gi 3/2,4-6
            201      community No    Gi 3/11-12
            202      community Yes   Gi 3/11-12
```

**Example (Primary)**

```
Dell# show vlan private-vlan primary
Primary Secondary Type      Active Ports
-----
10                primary Yes      Gi 2/1,3
20                primary Yes      Gi 3/1,3
```

**Example (Isolated)**

```
Dell# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
-----
10                primary Yes      Gi 2/1,3
                100      isolated Yes      Gi 2/2,4-6
                200      isolated Yes      Gi 3/2,4-6
```

**Example (Community)**

```
Dell# show vlan private-vlan community
Primary Secondary Type      Active Ports
-----
10                primary Yes      Gi 2/1,3
                101      community Yes      Gi 2/7-10
20                primary Yes      Po 10, 12-13
                Gi 3/1
                201      community No
                202      community Yes      Gi 3/11-12
```

**Example (Specific)**

```
Dell# show vlan private-vlan interface Gi 2/1
Primary Secondary Type      Active Ports
-----
10                primary Yes      Gi 2/1
```

**Usage Information**

If the VLAN ID is that of a primary VLAN, the entire private VLAN output is displayed, as shown below. If the VLAN ID is a secondary VLAN, only its primary VLAN and its particular secondary VLAN properties are displayed, as shown in the second Example.

**Example**

```
Dell# show vlan private-vlan 10
Primary Secondary Type      Active Ports
-----
10                primary Yes      Gi 2/1,3
                102      isolated Yes      Gi 0/4
                101      community Yes      Gi 2/7-10
```

**Example**

```
Dell# show vlan private-vlan 102
Primary Secondary Type      Active Ports
-----
10                Primary Yes      Po 1
                Gi 0/2
                102      Isolated Yes      Gi 0/4
```

**Related Commands**

- [private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.
- [show interfaces private-vlan](#) — displays type and status of PVLAN interfaces.
- [show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.
- [switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

## show vlan private-vlan mapping

Display primary-secondary VLAN mapping.

**Syntax** `show vlan private-vlan mapping`

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced the on MXL 10/40GbE Switch IO Module.

**Usage Information**

The output of this command, shown below, displays the community and isolated VLAN IDs that are associated with each primary VLAN.

**Example**

```
Dell# show vlan private-vlan mapping
Private Vlan:
  Primary      : 100
  Isolated    : 102
  Community   : 101
  Unknown     : 200
```

**Related Commands**

- [private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.
- [show vlan private-vlan](#) — displays type and status of PVLAN interfaces.
- [show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.
- [switchport mode private-vlan](#) — sets PVLAN mode of the selected port.

## switchport mode private-vlan

Set PVLAN mode of the selected port.

**Syntax**

```
[no] switchport mode private-vlan {host | promiscuous | trunk}
```

To remove PVLAN mode from the selected port, use the `no switchport mode private-vlan` command.

**Parameters**

<b>host</b>	Enter the keyword <code>host</code> to configure the selected port or port channel as an isolated interface in a PVLAN.
<b>promiscuous</b>	Enter the keyword <code>promiscuous</code> to configure the selected port or port channel as an promiscuous interface.
<b>trunk</b>	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

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown in the following example.

**Example**

```
Dell#conf
Dell(conf)#interface GigabitEthernet 2/1
Dell(conf-if-te-2/1)#switchport mode private-vlan promiscuous
```

```
Dell(conf)#interface GigabitEthernet 2/2
Dell(conf-if-te-2/2)#switchport mode private-vlan host

Dell(conf)#interface GigabitEthernet 2/3
Dell(conf-if-te-2/3)#switchport mode private-vlan trunk

Dell(conf)#interface port-channel 10
Dell(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

## Related Commands

[private-vlan mode](#) — sets the mode of the selected VLAN to community, isolated, or primary.

[private-vlan mapping secondary-vlan](#) — sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it.

[show interfaces private-vlan](#) — displays type and status of PVLAN interfaces.

[show vlan private-vlan mapping](#) — displays the primary-secondary VLAN mapping.

# Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking Operating System (OS) implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1w standard spanning tree protocol, but it creates a separate spanning tree for each VLAN configured.

**NOTE:** For easier command line entry, the plus (+) sign is not used at the command line.

## Topics:

- [description](#)
- [disable](#)
- [edge-port bpdufilter default](#)
- [extend system-id](#)
- [protocol spanning-tree pvst](#)
- [show spanning-tree pvst](#)
- [spanning-tree pvst](#)
- [spanning-tree pvst err-disable](#)
- [tc-flush-standard](#)
- [vlan bridge-priority](#)
- [vlan forward-delay](#)
- [vlan hello-time](#)
- [vlan max-age](#)

## description

Enter a description of the PVST+.

**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".)

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [protocol spanning-tree pvst](#) — enter SPANNING TREE mode on the switch.

## disable

Disable PVST+ globally.

**Syntax** `disable`  
To enable PVST+, use the `no disable` command.

**Defaults** Disabled.  
**Command Modes** CONFIGURATION (conf-pvst)  
**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [protocol spanning-tree pvst](#) — enter PVST+ mode.

## edge-port bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

**Syntax** `edge-port bpdufilter default`  
To disable global bpdu filter default, use the `no edge-port bpdufilter default` command.

**Defaults** Disabled  
**Command Modes** CONFIGURATION (The prompt is “config-pvst”.)  
**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

**Syntax** `extend system-id`  
**Defaults** Disabled  
**Command Modes** PROTOCOL PVST  
**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell(conf-pvst)#do show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID      Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
```

```

Interface                               Designated
Name  PortID  Prio Cost  Sts  Cost Bridge ID
PortID
-----
Po 23 128.24 128 1600 FWD 0 32768
001e.c9f1.00f3 128.24
Te 0/10 128.450 128 2000 DIS 0 32768
001e.c9f1.00f3 128.450
Te 0/11 128.459 128 2000 FWD 0 32768
001e.c9f1.00f3 128.459

Interface
Name      Role  PortID  Prio  Cost  Sts  Cost Link-type
Edge BpduFilter
-----
Po 23    Desg  128.24  128  1600  FWD  0    P2P No
No
Te 0/9   Dis   128.450 128  2000  DIS  0    P2P No
No
Te 0/10 Desg  128.459 128  2000  FWD  0    P2P No
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.

**Syntax** `protocol spanning-tree pvst`  
 To disable PVST+, use the `disable` command.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

- Syntax** `show spanning-tree pvst [vlan vlan-id] [brief] [guard]`
- Parameters**
- vlan *vlan-id*** (OPTIONAL) Enter the keyword `vlan` then the VLAN ID. The range is 1 to 4094.
  - brief** (OPTIONAL) Enter the keyword `brief` to view a synopsis of the PVST+ configuration information.
  - interface** (OPTIONAL) Enter one of the interface keywords along with the slot/port information:
    - For a Port Channel interface, enter the keyword `port-channel` then a number: The range is from 1 to 128.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` 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

**Supported Modes** Full—Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show spanning-tree pvst` command shown in the following examples.

Field	Description
<b>Interface Name</b>	PVST interface.
<b>Instance</b>	PVST instance.
<b>Sts</b>	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
<b>Guard Type</b>	Type of STP guard configured (Root, Loop, or BPDU guard).
<b>Bpdu Filter</b>	Yes - Bpdu filter Enabled No - Bpdu filter Disabled

## Example (Brief)

```
Dell# show spanning-tree pvst vlan 2 brief
VLAN 2
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 001e.c9f1.00f3
We are the root of Vlan 2
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally

Interface
Name      PortID  Prio  Cost  Sts  Cost  Designated
-----  -
Po 23    128.24  128   1600  FWD  0     32768 001e.c9f1.00f3 128.24
Te 0/10  128.450 128   2000  DIS  0     32768 001e.c9f1.00f3 128.450
Te 0/11  128.459 128   2000  FWD  0     32768 001e.c9f1.00f3 128.459
```

Interface							Bpdu		
Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge	Filter
Po 23	Desg	128.24	128	1600	FWD	0	P2P	No	No
Te 0/11	Dis	128.450	128	2000	DIS	0	P2P	No	No
Te 0/12	Desg	128.459	128	2000	FWD	0	P2P	No	No

### Example

```
Dell#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 32768, Address 001e.c9f1.00f3
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 32768, Address 001e.c9f1.00f3
Configured hello time 2, max age 20, forward delay 15
Bpdu filter disabled globally
We are the root of VLAN 2
Current root has priority 32768, Address 001e.c9f1.00f3
Number of topology changes 0, last change occurred 3dlh ago on

Port 24 (Port-channel 23) is designated Discarding
Port path cost 1600, Port priority 128, Port Identifier 128.24
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.24 , designated path cost 0
Number of transitions to forwarding state 0
BPDU sent 8, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 450 (TenGigabitEthernet 0/1) is disabled Discarding
Port path cost 2000, Port priority 128, Port Identifier 128.450
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.450 , designated path cost 0
Number of transitions to forwarding state 0
BPDU sent 0, received 0
The port is not in the Edge port mode, bpdu filter is disabled

Port 459 (TenGigabitEthernet 0/5) is designated Forwarding
Port path cost 2000, Port priority 128, Port Identifier 128.459
Designated root has priority 32768, address 001e.c9f1.00:f3
Designated bridge has priority 32768, address 001e.c9f1.00:f3
Designated port id is 128.459 , designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 16, received 0
The port is not in the Edge port mode, bpdu filter is disabled
```

### Example (EDS/ LBK)

```
Dell#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0

TenGigabitEthernet 0/1 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 0/2    128.1223 128  20000 EDS 0 32768 0001.e800.a12b 128.1223
```

### Example (EDS/ PVID)

```
Dell#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0

TenGigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
```

```
Bpdus sent 1, received 0

Interface Designated
Name      PortID   Prio Cost   Sts Cost Bridge ID           PortID
-----
Te 0/6 128.1223 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 Bpdu Filter
-----
Te 0/1 0      INCON(Root) Rootguard   No
Te 0/2 0      FWD      Loopguard   No
Te 0/3 0      EDS(Shut) Bpduguard   No
```

### 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.

**Syntax** `spanning-tree pvst {edge-port [bpduguard [shutdown-on-violation]] | bpdufilter} | err-disable | vlan vlan-range {cost number | priority value} | rootguard}`

### Parameters

<b>edge-port</b>	Enter the keywords <code>edge-port</code> to configure the interface as a PVST+ edge port.
<b>bpduguard</b>	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.
<b>shutdown-on-violation</b>	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
<b>bpdufilter</b>	(OPTIONAL) Enter the keyword <code>bpdufilter</code> to stop sending and receiving BPDUs on port fast enabled ports.
<b>err-disable</b>	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.
<b>vlan <i>vlan-range</i></b>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
<b>cost <i>number</i></b>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000.  Defaults: <ul style="list-style-type: none"> <li>• 10-Gigabit Ethernet interface = <b>2000</b>.</li> <li>• Port Channel interface with one 10 Gigabit Ethernet = <b>2000</b>.</li> <li>• Port Channel with two 10 Gigabit Ethernet = <b>1800</b>.</li> <li>• Port Channel with two 40 Mbps Ethernet = <b>600</b>.</li> </ul>
<b>priority <i>value</i></b>	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 <b>128</b> .
<b>rootguard</b>	Enter the keyword <code>rootguard</code> to enable root guard on a PVST+ port or port-channel interface.

**Defaults** Not configured.

**Command Modes** INTERFACE

**Supported Modes** Full—Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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. When BPDU guard and BPDU filter is enabled on the port, then BPDU filter takes the highest precedence.

**NOTE:** A port configured as an edge port, on a PVST switch, will immediately transition 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.

## Example

```
Dell(conf-if-te-0/1)#spanning-tree pvst vlan 3 cost 18000
Dell(conf-if-te-0/1)#end
Dell(conf-if-te-0/1)#show config
!
interface TenGigabitEthernet 0/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-te-0/1)#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.

**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

**Supported Modes** Full—Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, the system places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent the system from executing this action, use the `no spanning-tree pvst err-disable` command `cause invalid-pvst-bpdu`.

## Related Commands

[show spanning-tree pvst](#) — views the PVST+ configuration.

# tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

**Syntax** `tc-flush-standard`  
To disable, use the `no tc-flush-standard` command.

**Defaults** Disabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** By default, the system implements an optimized flush mechanism for PVST+. This implementation helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this *knob* command on to enable flushing MAC addresses after receiving every topology change notification.

# vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

**Syntax** `vlan vlan-id bridge-priority value`  
To return to the default value, use the `no vlan bridge-priority` command.

**Parameters**

- vlan *vlan-range*** Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
- bridge-priority *value*** Enter the keywords `bridge-priority` then the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

**Defaults** **32768**

**Command Modes** CONFIGURATION (conf-pvst)

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [vlan forward-delay](#) — changes the time interval before the system transitions to the Forwarding state.
- [vlan hello-time](#) — change the time interval between BPDUs.
- [vlan max-age](#) — changes the time interval before PVST+ refreshes.
- [show spanning-tree pvst](#) — displays the PVST+ configuration.

# vlan forward-delay

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

**Syntax** `vlan vlan-id forward-delay seconds`

To return to the default setting, use the `no vlan forward-delay` command.

<b>Parameters</b>	<b>vlan <i>vlan-range</i></b>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
	<b>forward-delay <i>seconds</i></b>	Enter the keywords <code>forward-delay</code> then the time interval, in seconds, that the system waits before transitioning PVST+ to the forwarding state. The range is from 4 to 30 seconds. The default is <b>15 seconds</b> .
<b>Defaults</b>	<b>15 seconds</b>	
<b>Command Modes</b>	CONFIGURATION (conf-pvst)	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">vlan bridge-priority</a> — sets the bridge-priority value.	
	<a href="#">vlan hello-time</a> — changes the time interval between BPDUs.	
	<a href="#">vlan max-age</a> — changes the time interval before PVST+ refreshes.	
	<a href="#">show spanning-tree pvst</a> — displays the PVST+ configuration.	

## vlan hello-time

Set the time interval between generation of PVST+ and BPDUs.

<b>Syntax</b>	<code>vlan <i>vlan-id</i> hello-time <i>seconds</i></code>
	To return to the default value, use the <code>no vlan hello-time</code> command.

<b>Parameters</b>	<b>vlan <i>vlan-range</i></b>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
	<b>hello-time <i>seconds</i></b>	Enter the keywords <code>hello-time</code> then the time interval, in seconds, between transmission of BPDUs. The range is from 1 to 10 seconds. The default is <b>2 seconds</b> .

<b>Defaults</b>	<b>2 seconds</b>	
<b>Command Modes</b>	CONFIGURATION (conf-pvst)	
<b>Supported Modes</b>	Full—Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Related Commands</b>	<a href="#">vlan bridge-priority</a> — sets the bridge-priority value.	
	<a href="#">vlan forward-delay</a> — changes the time interval before the system transitions to the forwarding state.	
	<a href="#">vlan max-age</a> — changes the time interval before PVST+ refreshes.	
	<a href="#">show spanning-tree pvst</a> — displays the PVST+ configuration.	

# vlan max-age

To maintain configuration information before refreshing that information, set the time interval for the PVST+ bridge.

**Syntax** `vlan vlan-range max-age seconds`

To return to the default, use the `no vlan max-age` command.

**Parameters**

- vlan *vlan-range*** Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
- max-age *seconds*** Enter the keywords `max-age` then the time interval, in seconds, that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

**Defaults** **20 seconds**

**Command Modes** CONFIGURATION (conf-pvst)

**Supported Modes** Full—Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [vlan bridge-priority](#) — sets the bridge-priority value.
- [vlan forward-delay](#) — changes the time interval before the system transitions to the forwarding state.
- [vlan hello-time](#) — changes the time interval between BPDUs.
- [show spanning-tree pvst](#) — displays the PVST+ configuration.

# 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.

## Topics:

- [Global Configuration Commands](#)
- [Per-Port QoS Commands](#)
- [Policy-Based QoS Commands](#)

## Global Configuration Commands

There are only two global configuration QoS commands.

### qos-rate-adjust

By default, while rate limiting, policing, and shaping, the system does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

<b>Syntax</b>	<code>qos-rate-adjustment <i>overhead-bytes</i></code>	
<b>Parameters</b>	<b><i>overhead-bytes</i></b>	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.
<b>Defaults</b>	QoS rate adjustment is disabled by default, and <code>no qos-rate-adjust</code> is listed in the running-configuration	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

<b>Syntax</b>	<code>service-class dot1p-mapping {dot1p0 <i>value</i>   dot1p1 <i>value</i>   dot1p2 <i>queue</i>   dot1p3 <i>value</i>   dot1p4 <i>value</i>  dot1p5 <i>value</i>   dot1p6 <i>value</i>   dot1p7 <i>value</i>}</code>	
<b>Parameters</b>	<b>value</b>	Enter a dot1p list number and value. The list number range is from 0 to 7. The range is from 0 to 3.
<b>Defaults</b>	For each dot1p Priority, the default CoS queue value is: <ul style="list-style-type: none"> <li>• dot1p CoS Queue <ul style="list-style-type: none"> <li>0 0-7</li> </ul> </li> </ul>	



1 0-7  
2 0-7  
3 0-7  
4 0-7  
5 0-7  
6 0-7  
7 0-7

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

## 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** `dot1p-priority priority-value`

To delete the IEEE 802.1p configuration on the interface, use the `no dot1p-priority` command.

**Parameters** *priority-value* Enter a value from 0 to 7.

<b>dot1p</b>	<b>Queue Number</b>
<b>0</b>	2
<b>1</b>	0
<b>2</b>	1
<b>3</b>	3
<b>4</b>	4
<b>5</b>	5
<b>6</b>	6
<b>7</b>	7

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	<p>The <code>dot1p-priority</code> 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.</p> <p>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 <code>dot1p-priority</code> command to individual interfaces in a port channel.</p>	

## rate police

Police the incoming traffic rate on the selected interface.

**Syntax** `rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]`


<b>Parameters</b>	<b>kbps</b>	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).
	<b>committed-rate</b>	Enter the bandwidth in Mbps. The range is from 0 to 10000.
	<b>burst-KB</b>	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is <b>50</b> .
	<b>peak peak-rate</b>	(OPTIONAL) Enter the keyword <code>peak</code> then a number to specify the peak rate in Mbps. The range is from 0 to 10000.
	<b>vlan vlan-id</b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

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.

For each physical interface, you can configure three `rate police` commands specifying different VLANs.

**Related Commands** [rate-police](#) — specifies traffic policing on the selected interface.

## rate-shape

Shape the traffic output on the selected interface.

**Syntax** `rate shape [kbps] 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).
- rate** Enter the outgoing rate in multiples of 10 Mbps. The range is from 10 to 10000.
- 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** QOS-POLICY-OUT

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you apply `rate-shape` in QoS policy both on the Queue Level and in Aggregate mode, the queue-based shaping occurs first then aggregate rate shaping.

## 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.

**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
<b>0</b>	0
<b>1</b>	0
<b>2</b>	0
<b>3</b>	1
<b>4</b>	2
<b>5</b>	3
<b>6</b>	3
<b>7</b>	3

**Command Modes**

- INTERFACE
- CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)

Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

## service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

**Syntax** `service-class bandwidth-percentage queue0 number queue1 number queue2 number queue3 number`

**Parameters** *number* Enter the bandwidth-weight, as a percentage. The range is from 1 to 100.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

#### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

Guarantee a minimum bandwidth to different queues globally using the `service-class bandwidth-percentage` command from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-percentage` command in an output QoS policy. The `bandwidth-percentage` command in QOS-POLICY-OUT mode supersedes the `service-class bandwidth-percentage` command.

When you enable ETS, the egress QoS features in the output QoS policy-map (such as `service-class bandwidth-percentage` and `bandwidth-percentage`), the default bandwidth allocation ratio for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Therefore, Dell Networking OS recommends disabling ETS when you wish to apply these features exclusively. After you disable ETS on an interface, the configured parameters are applied.

## strict-priority unicast

Configure a unicast queue as a strict-priority (SP) queue.

**Syntax** `strict-priority unicast queue number`

**Parameters** **unicast number** Enter the keyword `unicast` then the queue number. The range is from 1 to 3.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** After you configure a unicast queue as strict-priority, that particular queue, on the entire chassis, is treated as a `strict-priority 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. To assign the strict priority schedule type to egress queues, use the `scheduler strict` command in QOS-POLICY-OUT mode. The system OS does not support bandwidth configuration on strict priority scheduler queues.

When you enable ETS, the egress QoS features in the output QoS policy-map (such as `strict priority unicast <0-3>` and `scheduler strict`), default scheduler for egress queues are superseded by ETS configurations. This is to provide compatibility with DCBX. Therefore, Dell Networking OS recommends disabling ETS when you wish to apply these features exclusively. After you disable ETS on an interface, the configured parameters are applied.

## Policy-Based QoS Commands

Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or Loopbacks.

The commands are:

- [show qos dcb-map](#)
- [show qos dot1p-queue-mapping](#)

## bandwidth-percentage

Assign a percentage of weight to the class/queue.

**Syntax** `bandwidth-percentage percentage`

To remove the bandwidth percentage, use the `no bandwidth-percentage` command.

**Parameters** **percentage** Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).

**Defaults** none

**Command Modes** CONFIGURATION (conf-qos-policy-out)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The unit of bandwidth percentage is 1%. A bandwidth percentage of 0 is allowed and disables the scheduling of that class. 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.

## class-map

Create/access a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

**Syntax**

```
class-map {match-all | match-any} class-map-name [layer2]
```

**Parameters**

<b>match-all</b>	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords <code>match-all</code> to determine that the packets must meet all the match criteria in order to be a member of the class.
<b>match-any</b>	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.
<b>class-map-name</b>	Enter a name of the class for the class map in a character format (32 character maximum).
<b>layer2</b>	Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is <b>Layer 3</b> .

**Defaults**

Layer 3

**Command Modes**

CONFIGURATION

**Supported Modes**

Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Packets arriving at the input interface are checked against the match criteria 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 ip 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

Clears matched packets.

**Syntax** `clear qos statistics interface-name`

**Parameters** **interface-name** Enter one of the following keywords:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you issue this command, statistical information stored regarding QoS clears and resets to 0. You can access these statistics using the `show qos statistics` command in EXEC mode. When the traffic pattern matches the QoS classification criteria flows, the corresponding counters increment.

**Related Commands** [show qos statistics](#) — displays the QoS statistics.

## 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

**Supporting Modes** Full-Switch

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

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

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, MXL

## 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.

<b>Syntax</b>	<code>ip ssh rekey [time rekey-interval] [volume rekey-limit]</code> To reset to the default, use <code>no ip ssh rekey [time rekey-interval] [volume rekey-limit]</code> command.				
<b>Parameters</b>	<table><tr><td><b>time minutes</b></td><td>Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes</td></tr><tr><td><b>volume rekey-limit</b></td><td>Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b></td></tr></table>	<b>time minutes</b>	Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes	<b>volume rekey-limit</b>	Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b>
<b>time minutes</b>	Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes				
<b>volume rekey-limit</b>	Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b>				
<b>Defaults</b>	The default time is <b>60</b> minutes. The default volume is <b>1024</b> megabytes.				
<b>Command Modes</b>	CONFIGURATION mode				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, MXL

## match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

<b>Syntax</b>	<code>match ip access-group access-group-name [set-ip-dscp value]</code> To remove ACL match criteria from a class map, use the <code>no match ip access-group access-group-name [set-ip-dscp value]</code> command.						
<b>Parameters</b>	<table><tr><td><b>access-group-name</b></td><td>Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the <code>class-map</code> specifies.</td></tr><tr><td><b>set-ip-dscp value</b></td><td>(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.</td></tr></table>	<b>access-group-name</b>	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the <code>class-map</code> specifies.	<b>set-ip-dscp value</b>	(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.		
<b>access-group-name</b>	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the <code>class-map</code> specifies.						
<b>set-ip-dscp value</b>	(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.						
<b>Defaults</b>	none						
<b>Command Modes</b>	CLASS-MAP CONFIGURATION ( <code>config-class-map</code> )						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM..</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM..	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM..						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	To access this command, enter the <code>class-map</code> command. After the class map is identified, you can configure the match criteria. For <code>class-map match-any</code> , a maximum of five ACL match criteria are allowed. For <code>class-map match-all</code> , only one ACL match criteria is allowed.						
<b>Related Commands</b>	<a href="#">class-map</a> — identifies the class map.						



## match ip vlan

Uses a VLAN as the match criterion for an L3 class map.

**Syntax** `match ip vlan vlan-id`

To remove VLAN as the match criterion, use the `no match ip vlan vlan-id` command.

**Parameters** **vlan *vlan-id*** Enter the keyword `vlan` and then the ID of the VLAN. The range is from 1 to 4094.

**Defaults** none

**Command Modes** CONF-CLASS-MAP

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Introduced on the MXL switch.

**Usage Information** To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Use this command to match an IP class-map against a single VLAN ID .

**Related Commands** [class-map](#) — identifies the class map.

## match ip vrf

Uses a VRF as the match criterion for an L3 class map.

**Syntax** `match ip vrf vrf-id`

To remove VRF as the match criterion, use the `no match ip vrf vrf-id` command.

**Parameters** **vlan *vlan-id*** Enter the keyword `vrf` and then the ID of the VRF. The range is from 1 to 63.

**Defaults** none

**Command Modes** CONF-CLASS-MAP

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Introduced on the MXL switch.

**Usage Information** To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Use this command to match an IP class-map against a single VRF ID .

**Related Commands** [class-map](#) — identifies the class map.

## description

Add a description to the selected policy map or QoS policy.

<b>Syntax</b>	<code>description {description}</code> To remove the description, use the <code>no description {description}</code> command.										
<b>Parameters</b>	<b>description</b> Enter a description to identify the policies (80 characters maximum).										
<b>Defaults</b>	none										
<b>Command Modes</b>	CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)										
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch										
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.4(0.0)</td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.4(0.0)	Supported on the FN I/O Aggregator.	9.2(0.0)	Introduced on the M I/O Aggregator.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description										
9.9(0.0)	Introduced on the FN IOM.										
9.4(0.0)	Supported on the FN I/O Aggregator.										
9.2(0.0)	Introduced on the M I/O Aggregator.										
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.										
<b>Related Commands</b>	<a href="#">policy-map-output</a> — creates an output policy map. <a href="#">qos-policy-output</a> — creates an output QoS-policy on the router.										

## match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.


<b>Syntax</b>	<code>match {ip   ipv6   ip-any} dscp dscp-list [set-ip-dscp value]</code> To remove a DSCP value as a match criteria, use the <code>no match {ip   ipv6   ip-any} dscp dscp-list [[multicast] set-ip-dscp value]</code> command.								
<b>Parameters</b>	<b>ip</b> Enter the keyword <code>ip</code> to support IPv4 traffic. <b>ipv6</b> Enter the keyword <code>ipv6</code> to support IPv6 traffic <b>ip-any</b> Enter the keyword <code>ip-any</code> to support IPv4 and IPv6 traffic. <b>dscp-list</b> 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. <b>set-ip-dscp value</b> (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.								
<b>Defaults</b>	none								
<b>Command Modes</b>	CLASS-MAP CONFIGURATION (config-class-map)								
<b>Supported Modes</b>	Full-Switch								
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>9.5(0.0)</td><td>Introduced the <b>ipv6</b> and <b>ip-any</b> options on the MXL 10/40GbE Switch.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.5(0.0)	Introduced the <b>ipv6</b> and <b>ip-any</b> options on the MXL 10/40GbE Switch.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description								
9.9(0.0)	Introduced on the FN IOM.								
9.5(0.0)	Introduced the <b>ipv6</b> and <b>ip-any</b> options on the MXL 10/40GbE Switch.								
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.								

## 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.

## 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

<b>ip</b>	Enter the keyword <code>ip</code> to support IPv4 traffic.
<b>ipv6</b>	Enter the keyword <code>ipv6</code> to support IPv6 traffic.
<b>ip-any</b>	Enter the keyword <code>ip-any</code> to support IPv4 and IPv6 traffic.
<b>ip-precedence-list</b>	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.
<b>set-ip-dscp value</b>	(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)

## Supported Modes

Full-Switch

## Command History


Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.5(0.0)</b>	Introduced the support for <code>ipv6</code> and <code>ip-any</code> options on the MXL 10/40GbE Switch.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `match mac vlan number`

**Parameters** *number* Enter the VLAN ID. The range is from 1 to 4094.

**Defaults** none

**Command Modes** CLASS-MAP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To access this command, enter the `class-map` command. You can match against only one VLAN ID.

**Related Commands** [class-map](#) — identifies the class map.

## policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

<b>Syntax</b>	<code>policy-aggregate qos-policy-name</code>
	To remove a policy aggregate configuration, use the <code>no policy-aggregate qos-policy-name</code> command.
<b>Parameters</b>	<b><i>qos-policy-name</i></b> Enter the name of the policy map in character format (32 characters maximum).
<b>Defaults</b>	none
<b>Command Modes</b>	CONFIGURATION (policy-map-input and policy-map-output)
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can coexist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) apply. Any marking configurations in aggregate input QoS policy are ignored.
2. If aggregate input QoS policy and per class input QoS policy coexist, aggregate input QoS policy preempts per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in the aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

**Related Commands** [policy-map-output](#) — creates an output policy map.

## policy-map-input

Create an input policy map.

<b>Syntax</b>	<code>policy-map-input policy-map-name [layer2]</code>
	To remove an input policy map, use the <code>no policy-map-input policy-map-name [layer2]</code> command.
<b>Parameters</b>	<b><i>policy-map-name</i></b> Enter the name of the policy map in character format (32 characters maximum).

**layer2** (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

**Defaults** **Layer 3**

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
---------	-------------

<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.
- [policy-aggregate](#) — allows an aggregate method of configuring per-port QoS using policy maps.
- [service-policy input](#) — applies an input policy map to the selected interface.

## policy-map-output

Create an output policy map.

**Syntax** `policy-map-output policy-map-name`  
To remove a policy map, use the `no policy-map-output policy-map-name` command.

**Parameters** ***policy-map-name*** Enter the name for the policy map in character format (32 characters maximum).

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
---------	-------------

<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (`conf-policy-map-out`).

**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.

<b>Syntax</b>	<code>qos-policy-input qos-policy-name [layer2]</code> To remove an existing input QoS policy from the router, use the <code>no qos-policy-input qos-policy-name [layer2]</code> command.								
<b>Parameters</b>	<b>qos-policy-name</b> Enter the name for the policy map in character format (32 characters maximum). <b>layer2</b> (OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is <b>Layer 3</b> .								
<b>Defaults</b>	<b>Layer 3</b>								
<b>Command Modes</b>	CONFIGURATION								
<b>Supported Modes</b>	Full-Switch								
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the M I/O Aggregator.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.								
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.								
<b>Usage Information</b>	To specify the name of the input QoS policy, use this command. After the input policy is specified, <code>rate-police</code> is defined. This command enables QoS-Policy-Input Configuration mode — ( <code>conf-qos-policy-in</code> ).  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 <code>show qos statistics</code> command is reset.								
<b>Related Commands</b>	<a href="#">rate police</a> — incoming traffic policing function.								

## qos-policy-output

Create a QoS output policy.

<b>Syntax</b>	<code>qos-policy-output qos-policy-name</code> To remove an existing output QoS policy, use the <code>no qos-policy-output qos-policy-name</code> command.										
<b>Parameters</b>	<b>qos-policy-name</b> Enter your output QoS policy name in character format (32 characters maximum).										
<b>Defaults</b>	none										
<b>Command Modes</b>	CONFIGURATION										
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch										
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the M I/O Aggregator.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description										
<b>9.9(0.0)</b>	Introduced on the FN IOM.										
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.										
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.										
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.										

### Usage Information

To specify the name of the output QoS policy, use this command. After the output policy is specified, rate-limit, bandwidth-percentage, and WRED can be defined. This command enables QoS-Policy-Output Configuration mode — (conf-qos-policy-out).

### Related Commands

[bandwidth-percentage](#) — assigns weight to the class/queue percentage.

## rate police

Police the incoming traffic rate on the selected interface.

**Syntax** `rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB] ]`

### Parameters

<b>kbps</b>	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).
<b>committed-rate</b>	Enter the bandwidth in Mbps. The range is from 0 to 10000.
<b>burst-KB</b>	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is <b>100</b> .
<b>peak peak-rate</b>	(OPTIONAL) Enter the keyword <code>peak</code> then a number to specify the peak rate in Mbps. The range is from 0 to 10000. The default is the same as designated for <code>committed-rate</code> .

**Defaults** Burst size is 100 KB. `peak-rate` is the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Related Commands

[rate police](#) — specifies traffic policing on the selected interface.  
[qos-policy-input](#) — creates a QoS output policy.

## rate shape

Shape the traffic output on the selected interface.

**Syntax** `rate shape [kbps] rate [burst-KB]`

### Parameters

<b>kbps</b>	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).
<b>rate</b>	Enter the outgoing rate in multiples of 10 Mbps. The range is from 10 to 10000.
<b>burst-KB</b>	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is <b>50</b> .

**Defaults** Granularity for rate is **Mbps** unless you use the `kbps` option.

**Command Modes** QOS-POLICY-OUT

**Supported Modes** Full-Switch



<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the M I/O Aggregator.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	When you apply <code>rate-shape</code> in QoS policy both on the Queue Level and in Aggregate mode, the queue-based shaping occurs first then aggregate rate shaping.	

## service-policy input

Apply an input policy map to the selected interface.

**Syntax** `service-policy input policy-map-name [layer2]`

To remove the input policy map from the interface, use the `no service-policy input policy-map-name [layer2]` command.

**Parameters**

**policy-map-name** Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

**layer2** (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.


**Defaults** Layer 3

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	9.9(0.0)	Introduced on the FN IOM.
	9.2(0.0)	Introduced on the M I/O Aggregator.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

 **NOTE:** The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface.

**Related Commands** [policy-map-input](#) — creates an input policy map.

## service-policy output

Apply an output policy map to the selected interface.

**Syntax** `service-policy output policy-map-name`

To remove the output policy map from the interface, use the `no service-policy output policy-map-name` command.

**Parameters**

**policy-map-name** Enter the name for the policy map in character format (16 characters maximum). You can identify an existing policy map or name one that does not yet exist.

**Defaults** none

**Command Modes** INTERFACE

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.


**Related Commands** [policy-map-output](#) — creates an output policy map.

## service-queue

Assign a class map and QoS policy to different queues.

**Syntax** `service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]`

To remove the queue assignment, use the `no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]` command.

<b>Parameters</b>		
<b>queue-id</b>		Enter the value used to identify a queue. The range is from 0 to 3 (four queues per interface; four queues are reserved for control traffic).
<b>class-map class-map-name</b>	(OPTIONAL)	Enter the keyword <code>class-map</code> then the class map name assigned to the queue in character format (32 character maximum).  <b>NOTE:</b> This option is available under <code>policy-map-input</code> only.
<b>qos-policy qos-policy-name</b>	(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)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command assigns a class map or QoS policy to different queues.

**Related Commands** [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.

**Syntax** `set {ip-dscp value | mac-dot1p value}`

**Parameters**

**ip-dscp value** (OPTIONAL) Enter the keywords `ip-dscp` then the IP DSCP value. The range is from 0 to 63.

**mac-dot1p value** Enter the keywords `mac-dot1p` then the dot1p value. The range is from 0 to 7.

**Defaults** none

**Command Modes** CONFIGURATION (conf-qos-policy-in)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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 dcb-map

Display the DCB parameters configured in a specified DCB map.

**Syntax** `show qos dcb-map map-name`

**Parameters**      *map-name*      Displays the PFC and ETS parameters configured in the specified map.

**Command Modes**    • EXEC  
                         • EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O aggregator.

**Usage Information**      Use the `show qos dcb-map` command to display the enhanced transmission selection (ETS) and priority-based flow control (PFC) parameters used to configure server-facing Ethernet ports.

The following table describes the `show qos dcb-map` output shown in the example below.

Field	Description
<b>State</b>	Complete: All mandatory DCB parameters are correctly configured. In progress: The DCB map configuration is not complete. Some mandatory parameters are not configured.
<b>PFC Mode</b>	PFC configuration in DCB map: On (enabled) or Off.
<b>PG</b>	Priority group configured in the DCB map.
<b>TSA</b>	Transmission scheduling algorithm used by the priority group: Enhanced Transmission Selection (ETS).
<b>BW</b>	Percentage of bandwidth allocated to the priority group.
<b>PFC</b>	PFC setting for the priority group: On (enabled) or Off.
<b>Priorities</b>	802.1p priorities configured in the priority group.

### Example

```
Dell# show qos dcb-map dcbmap2

State      :Complete
PfcMode:ON
-----
PG:0 TSA:ETS BW:50 PFC:OFF
Priorities:0 1 2 4 5 6 7

PG:1 TSA:ETS BW:50 PFC:ON
Priorities:3
```

**Related Commands**      `dcb-map` — creates a DCB map to configure PFC and ETS parameters and applies the PFC and ETS settings on Ethernet ports.

## show qos policy-map

View the QoS policy map information.

**Syntax**      `show qos policy-map {summary [interface] | detail [interface]}`

**Parameters**

<b>summary</b> <b><i>interface</i></b>	To view a policy map interface summary, enter the keyword <code>summary</code> and optionally one of the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>For a 10 Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul>
---	---

<b>detail <i>interface</i></b>	To view a policy map interface in detail, enter the keyword <code>detail</code> and optionally one of the following keywords and slot/port or number information:
--------------------------------	---

- For a 10 Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example (IPv4)**

```
Dell#show qos policy-map detail tengigabitethernet 0/0

Interface tenGigabitEthernet 0/4

Policy-map-input policy
Trust dffserv
Queue# Class-map-name Qos-policy-name
0      -                q0
1      CM1              q1
2      CM2              q2
3      CM3              q3
```

**Example (Summary IPv4)**

```
Dell#sho qos policy-map summary

Interface policy-map-input policy-map-output
Gi 4/1      PM1      -
Te 4/2      PM2      PMOut
Dell#
```

## show qos policy-map-input

View the input QoS policy map details.

**Syntax** `show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]`

- Parameters**
- policy-map-name** Enter the policy map name.
  - class class-map-name** Enter the keyword `class` then the class map name.
  - qos-policy-input qos-policy-name** Enter the keyword `qos-policy-input` then the QoS policy name.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 qos-policy-output

View the output QoS policy details.

**Syntax** `show qos qos-policy-output [qos-policy-name]`

**Parameters** ***qos-policy-name*** Enter the QoS policy name.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show qos qos-policy-output

Qos-policy-output qmap_out
Bandwidth-percentage 10
Qos-policy-output qmap_wg
Rate-shape 100 50
Wred yellow wy
Wred green wg
Dell#
```

## show qos qos-policy-input

View the input QoS policy details.

**Syntax** `show qos qos-policy-input [qos-policy-name]`

**Parameters** ***qos-policy-name*** Enter the QoS policy name.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

**Syntax** `show qos qos-policy-output [qos-policy-name]`

**Parameters** **qos-policy-name** Enter the QoS policy name.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#show qos qos-policy-output

Qos-policy-output qmap_out
Bandwidth-percentage 10
Qos-policy-output qmap_wg
Rate-shape 100 50
Wred yellow wy
Wred green wg
Dell#
```

## show qos statistics

View QoS statistics.

**Syntax** `show qos statistics {egress-queue [interface]} | {wred-profile [interface]} | [inte`

**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 or number 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 or number 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 or number information.

**Defaults** none

**Command Modes** • EXEC

- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.11(0.0)	Updated the show qos statistics egress-queue output to reflect per queue per port.
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Added the egress-queue keyword.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell#show qos statistics egress-queue fortyGigE 0/37

Interface Fo 0/37
Unicast/Multicast Egress Queue Statistics
-----
Queue# Q# Type TxPkts TxPkts/s TxBytes TxBytes/s DroppedPkts DroppedPkts/s
-----
0 UCAST 0 0 0 0 0 0
1 UCAST 0 0 0 0 0 0
2 UCAST 0 0 0 0 0 0
3 UCAST 0 0 0 0 0 0
4 UCAST 0 0 0 0 0 0
5 UCAST 0 0 0 0 0 0
6 UCAST 0 0 0 0 0 0
7 UCAST 5575 0 624366 217 0 0
8 MCAST 0 0 0 0 0 0
9 MCAST 0 0 0 0 0 0
10 MCAST 0 0 0 0 0 0
11 MCAST 0 0 0 0 0 0
12 MCAST 0 0 0 0 0 0
Dell#
```

## show qos wred-profile

View the WRED profile details.

**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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell#show qos wred-profile

Wred-profile-name min-threshold max-threshold
wred_drop 0 0
wred_teng_y 467 4671
wred_teng_g 467 4671
wred_fortyg_y 467 4671
wred_fortyg_g 467 4671
```



## test cam-usage

Checks the Input Policy Map configuration for the CAM usage.

**Syntax** `test cam-usage service-policy input policy-map stack-unit {[number | [all]]}`

**Parameters**

<b><i>policy-map</i></b>	Enter the policy map name.
<b><i>stack-unit number</i></b>	(OPTIONAL) Enter the keywords <code>stack-unit</code> then the stack-unit number.
<b><i>stack-unit all</i></b>	(OPTIONAL) Enter the keywords <code>stack-unit all</code> to indicate all the stack-units.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 linecard` command shown in the following example.

<b>Field</b>	<b>Description</b>
<b>stack-unit</b>	Indicates the line card slot number.
<b>Portpipe</b>	Indicates the portpipe number.
<b>CAM Partition</b>	The CAM space where the rules are added.
<b>Available CAM</b>	Indicates the free CAM space, in the partition, for the classification rules. <b>i</b> <b>NOTE:</b> 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.
<b>Estimated CAM per Port</b>	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface. <b>i</b> <b>NOTE:</b> 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.
<b>Status (Allowed ports)</b>	Indicates if the input policy map configuration on an interface belonging to a linecard/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.

**i** **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
(Allowed ports)				per Port	
0	0	L2ACL	500	200	
Allowed (2)	1	L2ACL	100	200	
Exception					
1	0	L2ACL	1000	200	
Allowed (5)	1	L2ACL	0	200	
Exception					
		...			
		...			
		...			
13	1	L2ACL	400	200	
Allowed (2)					
Dell#					

## trust

Specify dynamic classification (DSCP) or dot1p to trust.

**Syntax** `trust {diffserv [fallback] | dot1p [fallback]}`

**Parameters**

- diffserv** Enter the keyword `diffserv` to specify trust of DSCP markings.
- dot1p** Enter the keyword `dot1p` to specify trust dot1p configuration.
- fallback** Enter the keyword `fallback` to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

**Defaults** none

**Command Modes** CONFIGURATION (conf-policy-map-in)

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

**Table 2. Default Mapping**

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	MXL Switch Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	3	48–63
110XXX		Internetwork Control	3	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	2	32–47
011XXX	AF3	Flash	1	16–31
010XXX	AF2	Immediate	1	16–31

**Table 2. Default Mapping (continued)**

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	MXL Switch Internal Queue ID	DSCP/CP Decimal
001XXX	AF1	Priority	0	0–15
000XXX	BE (Best Effort)	Best Effort	0	0–15

## wred

Designate the WRED profile to yellow or green traffic.

**Syntax** `wred [{yellow | green} profile-name] ecn`  
 To remove the WRED drop precedence, use the `no wred {yellow | green} [profile-name]` command.

**Parameters**

**yellow | green** Enter the keyword `yellow` for yellow traffic. A DSCP value of xxx110 and xxx101 maps to yellow.  
 Enter the keyword `green` for `green` traffic. A DSCP value of xxx0xx maps to green.

**profile-name** Enter your WRED profile name in character format (16 character maximum). Or use one of the five pre-defined WRED profile names.  
 Pre-defined Profiles: `wred_drop`, `wred-ge_y`, `wred-ge_g`, `wred_teng_y`, `wred_teng_`.

**ecn** When you configure `wred ecn <cr>` command, instead of dropping the packets exponentially, Explicit Congestion Notification (ECN) marking is made on the packets.

**Defaults** none

**Command Modes** CONFIGURATION (conf-qos-policy-out)

**Supported Modes** Full–Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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).

**Syntax** `wred ecn`  
 To stop marking packets, use the `no wred ecn` command.

**Defaults** none

**Command Modes** CONFIGURATION (conf-qos-policy-out)

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.0.2.0	Introduced on the S6000.
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-profile

Create a WRED profile and name the profile.

**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 (16 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles.

Pre-defined Profiles: `wred_drop`, `wred-ge_y`, `wred_ge_g`, `wred_teng_y`, `wred_teng_g`.

**Defaults** The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined `wred_ge_g` values.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the M I/O Aggregator.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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).

## 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 `yellow` keyword. Traffic marked as yellow delivers traffic to the egress queue which either transmits the packet if it has available bandwidth or drops the packet due to no ability to send.
- Red** Enter the `red` keyword. Traffic marked as red is dropped.
- dscp-list** Enter a list of IP DSCP values. The `dscp-list` parameter specifies the full list of IP DSCP value(s) for the specified color. Each DSCP value in a list is separate values by commas – no spaces (1,2,3) or indicates a list of values separated by a hyphen (1-3). Range is 0 to 63.

**Defaults** None

**Command Modes** CONFIG-COLOR-MAP

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
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.

<b>Syntax</b>	<code>qos dscp-color-map map-name</code> To remove a color map, use the <code>no qos dscp-color-map map-name</code> command.								
<b>Parameters</b>	<b>map-name</b> Enter the name of the DSCP color map. The map name can have a maximum of 32 characters.								
<b>Defaults</b>	<b>None</b>								
<b>Command Modes</b>	CONFIGURATION								
<b>Supported Modes</b>	Full-Switch								
<b>Command History</b>	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><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.7(0.0)</b></td><td>Introduced on the S6000-ON.</td></tr><tr><td><b>9.5.0.0</b></td><td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.7(0.0)</b>	Introduced on the S6000-ON.	<b>9.5.0.0</b>	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.7(0.0)</b>	Introduced on the S6000-ON.								
<b>9.5.0.0</b>	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.								
<b>Usage Information</b>	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.								
<b>Example</b>	<pre>Dell(conf)#qos dscp-color-map mymap</pre>								
<b>Related Commands</b>	<a href="#">qos dscp-color-map</a> — 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 <a href="#">dscp</a> — 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.

<b>Syntax</b>	<code>dscp-color-policy color-map-profile-name</code> To remove a color policy map profile, use the <code>no dscp-color-policy color-map-profile-name</code> command.
<b>Parameters</b>	<b>color-map-profile-name</b> Enter the color map profile name. The name can have a maximum of 32 characters.
<b>Defaults</b>	<b>None</b>
<b>Command Modes</b>	CONFIG-INTERFACE
<b>Supported Modes</b>	Full-Switch
<b>Command History</b>	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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>Version 9.5.0.0</b>	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.

**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** `show qos dscp-color-policy {summary [interface] | detail {interface}}`

**Parameters**

- summary** Enter the `summary` keyword to display summary information about a color policy on one or more interfaces.
- Detail** Enter the `detail` 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

**Supported Modes** Full-Switch

**Command History**

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

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

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.5.0.0</b>	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

**Example**

**Related Commands**

[show qos dscp-color-map](#) — displays DSCP color maps

## show qos dscp-color-map

Display the DSCP color map for one or all interfaces.

**Syntax** `show qos dscp-color-map map-name`

**Parameters**

- map-name*** Enter the name of the color map.

**Defaults** **None**

**Command Modes** EXEC

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
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](#) — displays a DSCP Color Policy Configuration

## show qos dot1p-queue-mapping

View dot1p to queue mapping.

**Syntax** `show qos dot1p-queue-mapping`

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

#### Example

```
Dell#show qos dot1p-queue-mapping
Dot1p Priority : 0 1 2 3 4 5 6 7
                Queue : 0 0 0 1 2 3 3 3
Dell#
```

## trust

Specify dynamic classification (DSCP) or dot1p to trust.

**Syntax** `trust {diffserv [fallback]| dot1p [fallback]}`



<b>Parameters</b>	<b>diffserv</b>	Enter the keyword <code>diffserv</code> to specify trust of DSCP markings.
	<b>dot1p</b>	Enter the keyword <code>dot1p</code> to specify trust dot1p configuration.
	<b>fallback</b>	Enter the keyword <code>fallback</code> to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

**Defaults** none

**Command Modes** CONFIGURATION (conf-policy-map-in)

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information**

When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

**Table 3. Default Mapping**

<b>DSCP/CP hex Range (XXX)</b>	<b>DSCP Definition</b>	<b>Traditional IP Precedence</b>	<b>MXL Switch Internal Queue ID</b>	<b>DSCP/CP Decimal</b>
111XXX		Network Control	3	48–63
110XXX		Internetwork Control	3	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	2	32–47
011XXX	AF3	Flash	1	16–31
010XXX	AF2	Immediate	1	16–31
001XXX	AF1	Priority	0	0–15
000XXX	BE (Best Effort)	Best Effort	0	0–15

# Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking Operating System (OS) supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2).

The implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, refer to the *Dell Networking OS Configuration Guide*.

## Topics:

- [auto-summary](#)
- [clear ip rip](#)
- [debug ip rip](#)
- [default-information originate](#)
- [default-metric](#)
- [description](#)
- [distance](#)
- [distribute-list in](#)
- [distribute-list out](#)
- [ip poison-reverse](#)
- [ip rip receive version](#)
- [ip rip send version](#)
- [ip split-horizon](#)
- [maximum-paths](#)
- [neighbor](#)
- [network](#)
- [offset-list](#)
- [output-delay](#)
- [passive-interface](#)
- [redistribute](#)
- [redistribute ospf](#)
- [router rip](#)
- [show config](#)
- [show ip rip database](#)
- [show running-config rip](#)
- [timers basic](#)
- [version](#)

## auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

**Syntax**                    `auto-summary`  
To send sub-prefix routing information, use the `no auto-summary` command.

**Defaults**                 Enabled.

**Command Modes**        ROUTER RIP

**Supported Modes**      Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip rip

Update all the RIP routes in the routing table.

**Syntax** `clear ip rip`

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command triggers updates of the main RIP routing tables.

## debug ip rip

Examine RIP routing information for troubleshooting.

**Syntax** `debug ip rip [interface | database | events [interface] | packet [interface] | trigger]`

To turn off debugging output, use the `no debug ip rip` command.

Parameters		
<b>interface</b>	(OPTIONAL) Enter the interface type and ID as one of the following:	<ul style="list-style-type: none"> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
<b>database</b>	(OPTIONAL) Enter the keyword <code>database</code> to display messages when there is a change to the RIP database.	
<b>events</b>	(OPTIONAL) Enter the keyword <code>events</code> to debug only RIP protocol changes.	
<b>trigger</b>	(OPTIONAL) Enter the keyword <code>trigger</code> to debug only RIP trigger extensions.	

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

# default-information originate

Generate a default route for the RIP traffic.

**Syntax** `default-information originate [always] [metric metric-value] [route-map map-name]`

To return to the default values, use the `no default-information originate` command.

**Parameters**

- always** (OPTIONAL) Enter the keyword `always` to enable the switch software to always advertise the default route.
- metric *metric-value*** (OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 1 to 16. The default is **1**.
- route-map *map-name*** (OPTIONAL) Enter the keywords `route-map` then the name of a configured route-map.

**Defaults** Disabled. Metric: **1**.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>description {description}</code> To remove the description, use the <code>no description {description}</code> command.						
<b>Parameters</b>	<b>description</b> Enter a description to identify the RIP protocol (80 characters maximum).						
<b>Defaults</b>	none						
<b>Command Modes</b>	ROUTER RIP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<a href="#">router rip</a> — 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.

<b>Syntax</b>	<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.						
<b>Parameters</b>	<b>weight</b> Enter a number from 1 to 255 for the weight (for prioritization). The default is <b>120</b> . <b>ip-address</b> (OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric. <b>mask</b> If you enter an IP address, also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x). <b>prefix-name</b> (OPTIONAL) Enter a configured prefix list name.						
<b>Defaults</b>	weight = <b>120</b>						
<b>Command Modes</b>	ROUTER RIP						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.9(0.0)</td><td>Introduced on the FN IOM.</td></tr><tr><td>8.3.16.1</td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<a href="#">default-metric</a> — assigns one distance metric to all routes learned using the <code>redistribute</code> command.						

# distribute-list in

Configure a filter for incoming routing updates.

<b>Syntax</b>	<code>distribute-list prefix-list-name in [interface]</code>
---------------	--

To delete the filter, use the `no distribute-list prefix-list-name in` command.

#### Parameters

- prefix-list-name*** Enter the name of a configured prefix list.
- interface*** (OPTIONAL) Identifies the interface type slot/port as one of the following:
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults** Not configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [ip prefix-list](#) — enters PREFIX-LIST mode and configures a prefix list.

## distribute-list out

Configure a filter for outgoing routing updates.

**Syntax** `distribute-list prefix-list-name out [interface | bgp | connected | ospf | static]`

To delete the filter, use the `no distribute-list prefix-list-name out` command.

#### Parameters

- prefix-list-name*** Enter the name of a configured prefix list.
- interface*** (OPTIONAL) Identifies the interface type slot/port as one of the following:
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
- connected** (OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
- ospf** (OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
- static** (OPTIONAL) Enter the keyword `static` to filter manually configured routes.

**Defaults** Not configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `ip poison-reverse`  
To disable poison reverse, use the `no ip poison-reverse` command.

**Defaults** Disabled.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `ip rip receive version [1] [2]`  
To return to the default, use the `no ip rip receive version` command.

**Parameters**

<b>1</b>	(OPTIONAL) Enter the number 1 for RIP version 1.
<b>2</b>	(OPTIONAL) Enter the number 2 for RIP version 2.

**Defaults** **RIPv1** and **RIPv2**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `ip rip send version [1] [2]`  
To return to the default value, use the `no ip rip send version` command.

<b>Parameters</b>	<b>1</b>	(OPTIONAL) Enter the number 1 for RIP version 1. The default is RIPv1.
	<b>2</b>	(OPTIONAL) Enter the number 2 for RIP version 2.
<b>Defaults</b>	<b>RIPv1</b>	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full–Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	To enable the interface to send both version of RIP packets, use the <code>ip rip send version 1 2</code> command.	
<b>Related Commands</b>	<a href="#">ip rip receive version</a> — sets the RIP version for the interface to receive traffic. <a href="#">version</a> — 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.

<b>Syntax</b>	<code>ip split-horizon</code>	
	To disable split-horizon, use the <code>no ip split-horizon</code> command.	
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full–Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Related Commands</b>	<a href="#">ip poison-reverse</a> — sets the prefix for RIP routing updates.	

## maximum-paths

Set RIP to forward packets over multiple paths.

<b>Syntax</b>	<code>maximum-paths number</code>	
	To return to the default values, use the <code>no maximum-paths</code> commands.	
<b>Parameters</b>	<b>number</b>	Enter the number of paths. The range is from 1 to 16. The default is <b>4</b> paths.
<b>Defaults</b>	<b>4</b>	
<b>Command Modes</b>	ROUTER RIP	
<b>Supported Modes</b>	Full–Switch	



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** RIP supports a maximum of 16 ECMP paths.

## neighbor

Define a neighbor router with which to exchange RIP information.

**Syntax** `neighbor ip-address`  
To delete a neighbor setting, use the `no neighbor ip-address` command.

**Parameters** ***ip-address*** Enter the IP address, in dotted decimal format, of a router with which to exchange information.

**Defaults** Not configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible. To ensure that only specific interfaces are receiving and sending data, use the `passive-interface` command with the `neighbor` command.

**Related Commands** [passive-interface](#) — sets the interface to only listen to RIP broadcasts.

## network

Enable RIP for a specified network. To enable RIP on all networks connected to the switch, use this command.

**Syntax** `network ip-address`  
To disable RIP for a network, use the `no network ip-address` command.

**Parameters** ***ip-address*** Specify an IP network address in dotted decimal format. You cannot specify a subnet.

**Defaults** No RIP network is configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

## Syntax

```
offset-list prefix-list-name {in | out} offset [interface]
```

To delete an offset list, use the `no offset-list prefix-list-name {in | out} offset [interface]` command.

## Parameters

- prefix-list-name** Enter the name of an established Prefix list to determine which incoming routes are modified.
- offset** Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
- interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

## Defaults

Not configured.

## Command Modes

ROUTER RIP

## Supported Modes

Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

## Syntax

```
output-delay delay
```

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

## Parameters

**delay** Specify a number of milliseconds as the delay interval. The range is from 8 to 50.

## Defaults

Not configured.

## Command Modes

ROUTER RIP

## Supported Modes

Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is intended for low-speed interfaces.

## passive-interface

Suppress routing updates on a specified interface.

**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 information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults** Not configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `redistribute {connected | static}`  
 To disable redistribution, use the `no redistribute {connected | static}` command.

**Parameters**

**connected** Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.

**static** Enter the keyword `static` to specify that information from static routes is redistributed.

**Defaults** Not configured.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 ospf

Redistribute routing information from an OSPF process.

<b>Syntax</b>	<code>redistribute ospf process-id [match external {1   2}   match internal   metric metric-value] [route-map map-name]</code>	
	To disable redistribution, use the <code>no redistribute ospf process-id [match external {1   2}   match internal   metric metric-value] [route-map map-name]</code> command.	
<b>Parameters</b>	<b>process-id</b>	Enter a number that corresponds to the OSPF process ID to redistribute. The range is from 1 to 65355.
	<b>match external {1   2}</b>	(OPTIONAL) Enter the keywords <code>match external</code> then the numbers 1 or 2 to indicate that external 1 routes or external 2 routes should be redistributed.
	<b>match internal</b>	(OPTIONAL) Enter the keywords <code>match internal</code> to indicate that internal routes should be redistributed.
	<b>metric metric-value</b>	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 0 to 16.
	<b>route-map map-name</b>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of a configured route map.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	ROUTER RIP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## router rip

To configure and enable RIP, enter ROUTER RIP mode.

<b>Syntax</b>	<code>router rip</code>	
	To disable RIP, use the <code>no router rip</code> command.	
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To enable RIP, assign a network address using the `network` command.

**Example**

```
Dell(conf)#router rip
Dell(conf-router_rip)#
```

**Related Commands** `network` — enables RIP.

## show config

Display the changes you made to the RIP configuration. The default values are not shown.

**Syntax** `show config`

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-router_rip)#show config
!
router rip
  network 172.31.0.0
  passive-interface TenGigabitEthernet 0/1
Dell(conf-router_rip)#
```

## show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

**Syntax** `show ip rip database [ip-address mask]`

**Parameters**

- ip-address*** (OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, also enter a mask for that IP address.
- mask*** (OPTIONAL) Specify a mask, in `/network` format, for the IP address.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ip rip database` command shown in the following example.

Field	Description
<b>Total number of routes in RIP database</b>	Displays the number of RIP routes stored in the RIP database.
<b>100.10.10.0/24 directly connected</b>	Lists the routes directly connected.
<b>150.100.0.0 redistributed</b>	Lists the routes learned through redistribution.
<b>209.9.16.0/24...</b>	Lists the routes and the sources advertising those routes.

### Example

```
Dell#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
    [50/1] via 192.14.1.3, 00:00:12, TenGigabitEthernet 0/1
204.250.54.0/24    auto-summary
203.250.49.0/24
    [50/1] via 192.13.1.3, 00:00:12, TenGigabitEthernet 0/1
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.

**Syntax** show running-config rip

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
show running-config rip
!
router rip
  distribute-list Test1 in
  distribute-list Test21 out
  network 10.0.0.0
  passive-interface TenGigabitEthernet 1/4
  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.

**Syntax** `timers basic update invalid holddown flush`  
To return to the default settings, use the `no timers basic` command.

**Parameters**

- update*** Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is from zero (0) to 4294967295. The default is **30 seconds**.
- invalid*** Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
- holddown*** Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
- flush*** Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is from zero (0) to 4294967295. The default is **240 seconds**.

- Defaults**
- update = **30 seconds**
  - invalid = **180 seconds**
  - holddown = **180 seconds**
  - flush = **240 seconds**

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**Syntax** `version {1 | 2}`  
To return to the default version setting, use the `no version` command.

**Parameters**

- 1** Enter the keyword 1 to specify RIP version 1.
- 2** Enter the keyword 2 to specify RIP version 2.

**Defaults** The system sends RIPv1 and receives RIPv1 and RIPv2.

**Command Modes** ROUTER RIP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

<b>Version</b>	<b>Description</b>
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 System (OS) remote monitoring (RMON) is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection.

RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, RFC-3434 and RFC-4502:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819
- User History; RFC-4502
- Probe Configuration (Capabilities, SoftwareRev, HardwareRev, Date Time and ResetControl); RFC-4502

RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

**i** **NOTE:** Only simple network management protocol (SNMP) GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

## Topics:

- [rmon alarm](#)
- [rmon collection history](#)
- [rmon collection statistics](#)
- [rmon event](#)
- [rmon hc-alarm](#)
- [show rmon](#)
- [show rmon alarms](#)
- [show rmon events](#)
- [show rmon hc-alarm](#)
- [show rmon history](#)
- [show rmon log](#)
- [show rmon statistics](#)

## rmon alarm

Set an alarm on any MIB object.

**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.

<b><i>variable</i></b>	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.
<b><i>interval</i></b>	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.
<b><i>delta</i></b>	Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
<b><i>absolute</i></b>	Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
<b><i>rising-threshold value event-number</i></b>	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.
<b><i>falling-threshold value event-number</i></b>	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.
<b><i>owner string</i></b>	(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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

**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.

<b>Parameters</b>		
<b><i>controlEntry integer</i></b>	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.	
<b><i>owner name</i></b>	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to record the owner of the RMON group of statistics.	
<b><i>buckets number</i></b>	(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 <b>50</b> .	
<b><i>interval seconds</i></b>	(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 <b>1800 seconds</b> .	

**Defaults** none

**Command Modes** CONFIGURATION INTERFACE (config-if)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## rmon collection statistics

Enable RMON MIB statistics collection on an interface.

**Syntax** `rmon collection statistics {controlEntry integer} [owner name]`  
To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

**Parameters**

<b>controlEntry <i>integer</i></b>	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.
<b>owner <i>name</i></b>	(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)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## rmon event

Add an event in the RMON event table.

**Syntax** `rmon event number [log] [trap community] [description string] [owner name]`  
To disable RMON on an interface, use the `no rmon event number` command.

**Parameters**

<b><i>number</i></b>	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.
<b>log</b>	(OPTIONAL) Enter the keyword <code>log</code> to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is <b>No log</b> .
<b>trap <i>community</i></b>	(OPTIONAL) Enter the keyword <code>trap</code> then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either <code>snmp-trap</code> or <code>log-and-trap</code> . The default is <b>public</b> .
<b>description <i>string</i></b>	(OPTIONAL) Enter the keyword <code>description</code> then a string describing the event.
<b>owner <i>name</i></b>	(OPTIONAL) Enter the keyword <code>owner</code> then the name of the owner of this event.

**Defaults** As noted in the *Parameters* section.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## rmon hc-alarm

Set an alarm on any MIB object.

**Syntax** `rmon hc-alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]`

To disable the alarm, use the `no rmon hc-alarm number` command.

<b>Parameters</b>		
<b><i>number</i></b>		Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
<b><i>variable</i></b>		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.
<b><i>interval</i></b>		Time, in seconds, the alarm monitors the MIB variables; this is the <code>alarmSampleType</code> in the RMON alarm table. The range is from 5 to 3600 seconds.
<b><i>delta</i></b>		Enter the keyword <code>delta</code> to test the change between MIB variables. This is the <code>alarmSampleType</code> in the RMON alarm table.
<b><i>absolute</i></b>		Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the <code>alarmSampleType</code> in the RMON alarm table.
<b><i>rising-threshold value event-number</i></b>		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 <code>alarmRisingEventIndex</code> or <code>alarmTable</code> of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
<b><i>falling-threshold value event-number</i></b>		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 <code>alarmFallingEventIndex</code> or the <code>alarmTable</code> of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
<b><i>owner string</i></b>		(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to specify an owner for the alarm. This is the <code>alarmOwner</code> object in the <code>alarmTable</code> of the RMON MIB.

**Defaults** `owner`

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show rmon

Display the RMON running status including the memory usage.

**Syntax** `show rmon`

**Defaults** none  
**Command Modes** EXEC  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

**Syntax** show rmon alarms [*index*] [*brief*]

**Parameters**

- index*** (OPTIONAL) Enter the table index number to display just that entry.
- brief*** (OPTIONAL) Enter the keyword *brief* to display the RMON alarm table in an easy-to-read format.

**Defaults** none  
**Command Modes** EXEC  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

**Syntax** `show rmon events [index] [brief]`

**Parameters**

- index** (OPTIONAL) Enter the table index number to display just that entry.
- brief** (OPTIONAL) Enter the keyword `brief` to display the RMON event table in an easy-to-read format.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example (Index)

```

Dell#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
Dell#

```

### Example (Brief)

```

Dell#show rmon event br
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.

**Syntax** `show rmon hc-alarm [index] [brief]`

**Parameters**

- index*** (OPTIONAL) Enter the table index number to display just that entry.
- brief*** (OPTIONAL) Enter the keyword `brief` to display the RMON High-Capacity alarm table in an easy-to-read format.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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.

**Syntax** `show rmon history [index] [brief]`

**Parameters**

- index** (OPTIONAL) Enter the table index number to display just that entry.
- brief** (OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet history table in an easy-to-read format

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example (Index)

```
Dell#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
Dell#
```

## Example (Brief)

```
Dell#show rmon history brief
index      ifIndex      interface
-----
6001      100974631    GigabitEthernet 2/0
6002      100974631    GigabitEthernet 2/0
6003      101236775    GigabitEthernet 2/1
6004      101236775    GigabitEthernet 2/1
9001      134529054    GigabitEthernet 3/0
9002      134529054    GigabitEthernet 3/0
9003      134791198    GigabitEthernet 3/1
9004      134791198    GigabitEthernet 3/1
Dell#
```

# show rmon log

Display the contents of the RMON log table.

**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

**Supported Modes** Full-Switch



**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Example (Index)**

```
Dell#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 GigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
```

```

1024-1518 bytes packets: 0
owner: 1
status: OK
<high-capacity data>
HC packets received overflow: 0
HC packets received: 0
HC bytes received overflow: 0
HC bytes received: 0
HC 64bytes packets overflow: 0
HC 64bytes packets: 0
HC 65-127 bytes packets overflow: 0
HC 65-127 bytes packets: 0
HC 128-255 bytes packets overflow: 0
HC 128-255 bytes packets: 0
HC 256-511 bytes packets overflow: 0
HC 256-511 bytes packets: 0
HC 512-1023 bytes packets overflow: 0
HC 512-1023 bytes packets: 0
HC 1024-1518 bytes packets overflow: 0
HC 1024-1518 bytes packets: 0
Dell#

```

### Example (Brief)

```

Dell#show rmon statistics br
index      ifIndex      interface
-----
6001      100974631    GigabitEthernet 2/0
6002      100974631    GigabitEthernet 2/0
6003      101236775    GigabitEthernet 2/1
6004      101236775    GigabitEthernet 2/1
9001      134529054    GigabitEthernet 3/0
9002      134529054    GigabitEthernet 3/0
9003      134791198    GigabitEthernet 3/1
9004      134791198    GigabitEthernet 3/1
Dell#

```

# Rapid Spanning Tree Protocol (RSTP)

The Dell Networking Operating System (OS) implementation of rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

## Topics:

- [bridge-priority](#)
- [debug spanning-tree rstp](#)
- [description](#)
- [disable](#)
- [forward-delay](#)
- [hello-time](#)
- [max-age](#)
- [edge-port bpdufilter default](#)
- [protocol spanning-tree rstp](#)
- [show config](#)
- [spanning-tree rstp](#)
- [spanning-tree rstp](#)
- [tc-flush-standard](#)

## bridge-priority

Set the bridge priority for RSTP.

**Syntax** `bridge-priority priority-value`  
To return to the default value, use the `no bridge-priority` command.

**Parameters** `priority-value` Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

**Defaults** **32768**

**Command Modes** CONFIGURATION RSTP (conf-rstp)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Parameters</b>	<b>all</b>	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
	<b>bpdu <i>interface</i> {in   out}</b>	(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 options are the following: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul> Optionally, enter an <code>in</code> or <code>out</code> parameter with the optional interface: <ul style="list-style-type: none"> <li>• For Receive, enter <code>in</code>.</li> <li>• For Transmit, enter <code>out</code>.</li> </ul>
	<b>events</b>	(OPTIONAL) Enter the keyword <code>events</code> to debug RSTP events.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#debug spanning-tree rstp bpdu gigabitethernet 2/0 ?
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".)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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)  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 the system waits before transitioning RSTP to the forwarding state. The range is from 4 to 30. The default is **15 seconds**.

**Defaults** **15 seconds**

**Command Modes** CONFIGURATION RSTP (conf-rstp)  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 `milli-second` to configure a hello time on the order of milliseconds. The range is from 50 to 950 milliseconds

**Defaults** **2 seconds**

**Command Modes** CONFIGURATION RSTP (conf-rstp)  
**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.	
<b>Related Commands</b>	<a href="#">forward-delay</a> — changes the wait time before RSTP transitions to the Forwarding state.	
	<a href="#">max-age</a> — 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.

<b>Syntax</b>	<code>max-age seconds</code>	
	To return to the default values, use the <code>no max-age</code> command.	
<b>Parameters</b>	<b><i>max-age</i></b>	Enter a number of seconds that the waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is <b>20 seconds</b> .
<b>Defaults</b>	<b>20 seconds</b>	
<b>Command Modes</b>	CONFIGURATION RSTP (conf-rstp)	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Related Commands</b>	<a href="#">forward-delay</a> — changes the wait time before RSTP transitions to the Forwarding state.
	<a href="#">hello-time</a> — changes the time interval between BPDUs.

## edge-port bpdufilter default

To filter transmission of BPDU on port fast enabled interfaces, enable BPDU Filter globally.

<b>Syntax</b>	<code>edge-port bpdufilter default</code>	
	To disable global bpdu filter default, use the <code>no edge-port bpdufilter default</code> command.	
<b>Parameters</b>	<b><i>priority-value</i></b>	Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is <b>32768</b> .
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	CONFIGURATION (conf-rstp)	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes**   Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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)

**Supported Modes**   Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-rstp)#show config
!
protocol spanning-tree rstp
  no disable
  bridge-priority 16384
```

# 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.

<b>Syntax</b>	<code>spanning-tree rstp {cost <i>port-cost</i>   edge-port [bpduguard [shutdown-on-violation]]   bpdufilter   priority <i>priority</i>   {rootguard}}</code>	
<b>Parameters</b>	<b>cost <i>port-cost</i></b>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: <ul style="list-style-type: none"><li>• 10-Gigabit Ethernet interface = <b>2000</b></li><li>• Port Channel interface with one 10 Gigabit Ethernet = <b>2000</b></li><li>• Port Channel interface with one 40 Gigabit Ethernet = <b>1400</b></li><li>• Port Channel with two 10 Gigabit Ethernet = <b>1800</b></li><li>• Port Channel with two 40 Gigabit Ethernet = <b>600</b></li></ul>
	<b>edge-port</b>	Enter the keywords <code>edge-port</code> to configure the interface as a rapid spanning tree edge port.
	<b>bpduguard</b>	(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.
	<b>shutdown-on-violation</b>	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
	<b>bpdufilter</b>	(OPTIONAL) Enter the keyword <code>bpdufilter</code> to enable BPDU Filter to stop sending and receiving BPDUs on port enabled interfaces.
	<b>priority <i>priority</i></b>	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 <b>128</b> .
	<b>rootguard</b>	Enter the keyword <code>rootguard</code> to enable root guard on an RSTP port or port-channel interface.

**Defaults** Not configured.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 gigabitethernet 4/0
Dell(conf-if-gi-4/0)#spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)#show config
!
interface GigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

## 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** `spanning-tree rstp {cost port-cost | edge-port [bpduguard [shutdown-on-violation]] | bpdufilter | priority priority | {rootguard}}`

### Parameters

<b>cost <i>port-cost</i></b>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: <ul style="list-style-type: none"> <li>• 10-Gigabit Ethernet interface = <b>2000</b></li> <li>• Port Channel interface with one 10 Gigabit Ethernet = <b>2000</b></li> <li>• Port Channel interface with one 40 Gigabit Ethernet = <b>1400</b></li> <li>• Port Channel with two 10 Gigabit Ethernet = <b>1800</b></li> <li>• Port Channel with two 40 Gigabit Ethernet = <b>600</b></li> </ul>
<b>edge-port</b>	Enter the keywords <code>edge-port</code> to configure the interface as a rapid spanning tree edge port.
<b>bpduguard</b>	(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.
<b>shutdown-on-violation</b>	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
<b>bpdufilter</b>	(OPTIONAL) Enter the keyword <code>bpdufilter</code> to enable BPDU Filter to stop sending and receiving BPDUs on port enabled interfaces.
<b>priority <i>priority</i></b>	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 <b>128</b> .
<b>rootguard</b>	Enter the keyword <code>rootguard</code> to enable root guard on an RSTP port or port-channel interface.

**Defaults** Not configured.

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 gigabitethernet 4/0
Dell(conf-if-gi-4/0)#spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)#show config
!
interface GigabitEthernet 4/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

# tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

**Syntax** `tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

**Defaults** Disabled

**Command Modes** CONFIGURATION (conf-rstp)

**Supported Modes** Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

By default, the system implements an optimized flush mechanism for RSTP. This implementation helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this `knob` command to enable flushing MAC addresses after receiving every topology change notification.

# Security

This chapter describes various types of security commands in the Dell Networking OS, in the following sections:

The commands are listed in the following sections:

- [AAA Accounting Commands](#)
- [Authentication and Password Commands](#)
- [RADIUS Commands](#)
- [TACACS+ Commands](#)
- [SSH Server and SCP Commands](#)

**i** **NOTE:** Starting with the Dell Networking OS version 7.2.1.0, LEAP with MSCHAP v2 supplicant is implemented.

## Topics:

- [AAA Accounting Commands](#)
- [Authentication and Password Commands](#)
- [RADIUS Commands](#)
- [Suppressing AAA Accounting for Null Username Sessions](#)
- [TACACS+ Commands](#)
- [SSH Server and SCP Commands](#)
- [Secure DHCP Commands](#)
- [ICMP Vulnerabilities](#)
- [System Security Commands](#)

## 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} {name | default}{start-stop | wait-start | stop-only} {radius | tacacs+}`

To disable AAA Accounting, use the `no aaa accounting {system | exec | command level} {name | default}{start-stop | wait-start | stop-only} {radius | tacacs+} command`.

**Parameters**

<b>system</b>	Enter the keyword <code>system</code> to send accounting information of any other AAA configuration.
<b>exec</b>	Enter the keyword <code>exec</code> to send accounting information when a user has logged in to EXEC mode.
<b>commands level</b>	Enter the keyword <code>command</code> then a privilege level for accounting of commands executed at that privilege level.

<b>name   default</b>	Enter one of the following: <ul style="list-style-type: none"> <li>For <code>name</code>, enter a user-defined name of a list of accounting methods.</li> <li>For <code>default</code>, the default accounting methods used.</li> </ul>
<b>start-stop</b>	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.
<b>wait-start</b>	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.
<b>stop-only</b>	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.
<b>radius</b>	Enter the keyword <code>radius</code> to use RADIUS service for exec and dot1x accounting.
<b>tacacs+</b>	Enter the keyword <code>tacacs+</code> to use TACACS+ data for accounting. Dell Networking OS currently only supports TACACS+ accounting.

**Defaults** none  
**Command Modes** CONFIGURATION  
**Supported Modes** All Modes

Command History	Version	Description
	<b>9.14(1.5)</b>	Added support for RADIUS accounting.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator and M I/O Aggregator.

**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 (TACACS+)**

```
DellEMC(conf)# aaa accounting exec default start-stop tacacs+
DellEMC(conf)# aaa accounting command 15 default start-stop tacacs+
DellEMC(conf)# aaa accounting command role secaadmin default start-stop tacacs+
```

**Example (RADIUS)**

```
DellEMC(conf)# aaa accounting dot1x default start-stop radius
DellEMC(conf)# aaa accounting dot1x default stop-only radius
```

**Related Commands** [enable password](#) — changes the password for the `enable` command.

## 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

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator and M I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator and M I/O Aggregator.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator and M I/O Aggregator.						
<b>Usage Information</b>	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 <code>aaa authentication login method-list none</code> command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the <code>aaa accounting suppress</code> command.						

## aaa authorization commands

Set parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands.

<b>Syntax</b>	<pre>aaa authorization commands {level}{name default} {local   tacacs+  none}</pre> <p>Undo a configuration with the <code>no aaa authorization commands {level}{name default} {local   tacacs+   none}</code> command.</p>												
<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b>commands level</b></td> <td>Enter the keyword <code>commands</code> then the command privilege level for command level authorization.</td> </tr> <tr> <td style="vertical-align: top;"><b>name</b></td> <td>Define a name for the list of authorization methods.</td> </tr> <tr> <td style="vertical-align: top;"><b>default</b></td> <td>Define the default list of authorization methods.</td> </tr> <tr> <td style="vertical-align: top;"><b>local</b></td> <td>Use the authorization parameters on the system to perform authorization.</td> </tr> <tr> <td style="vertical-align: top;"><b>tacacs+</b></td> <td>Use the TACACS+ protocol to perform authorization.</td> </tr> <tr> <td style="vertical-align: top;"><b>none</b></td> <td>Enter the keyword <code>none</code> to apply no authorization.</td> </tr> </table>	<b>commands level</b>	Enter the keyword <code>commands</code> then the command privilege level for command level authorization.	<b>name</b>	Define a name for the list of authorization methods.	<b>default</b>	Define the default list of authorization methods.	<b>local</b>	Use the authorization parameters on the system to perform authorization.	<b>tacacs+</b>	Use the TACACS+ protocol to perform authorization.	<b>none</b>	Enter the keyword <code>none</code> to apply no authorization.
<b>commands level</b>	Enter the keyword <code>commands</code> then the command privilege level for command level authorization.												
<b>name</b>	Define a name for the list of authorization methods.												
<b>default</b>	Define the default list of authorization methods.												
<b>local</b>	Use the authorization parameters on the system to perform authorization.												
<b>tacacs+</b>	Use the TACACS+ protocol to perform authorization.												
<b>none</b>	Enter the keyword <code>none</code> to apply no authorization.												
<b>Defaults</b>	none												
<b>Command Modes</b>	CONFIGURATION												
<b>Supported Modes</b>	All Modes												
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell Networking OS version history for this command.</p> <table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.6.(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.						
<b>Version</b>	<b>Description</b>												
<b>9.9(0.0)</b>	Introduced on the FN IOM.												
<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.												

## aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

<b>Syntax</b>	<pre>aaa authorization config-commands</pre> <p>Disable authorization checking for CONFIGURATION level commands using the <code>no aaa authorization config-commands</code> command.</p>
<b>Defaults</b>	Enabled when you configure <code>aaa authorization commands</code> command.
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	All Modes

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

The following table lists the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6.(0.0)	Supported on the FN I/O Aggregator and M I/O Aggregator.

**Usage Information** By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. Use the command `no aaa authorization config-commands` to enable only EXEC-level command checking.

## aaa authorization exec

Set parameters that restrict (or permit) a user's access to EXEC-level commands.

**Syntax** `aaa authorization exec {name | default} {local || tacacs+ || if-authenticated || none}`

To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

**Parameters**

- name** Define a name for the list of authorization methods.
- default** Define the default list of authorization methods.
- local** Use the authorization parameters on the system to perform authorization.
- tacacs+** Use the TACACS+ protocol to perform authorization.
- none** Enter the keyword `none` to apply no authorization.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

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

The following table lists the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6.(0.0)	Supported on the FN I/O Aggregator and M I/O Aggregator.

## accounting

Apply an accounting method list to terminal lines.

**Syntax** `accounting {exec | commands {level | role role-name} method-list}`

**Parameters**

- exec** Enter the keyword `exec` to apply an EXEC level accounting method list.
- commands {level | role role-name}** Enter the keywords `commands level` to apply an EXEC and CONFIGURATION level accounting method list or enter the keywords `commands role` and then the role name for accounting of commands run by a user with that role.
- method-list** Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting commands`.

**Defaults** none  
**Command Modes** LINE  
**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator and M I/O Aggregator.

**Related Commands** [aaa accounting](#) — enables AAA Accounting and creates a record for monitoring the accounting function.

**Example** The following example configures accounting for the role `secadmin` using default method:

```
Dell(conf-vty-0)# accounting commands role secadmin default
```

## 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

**Supporting Modes** Full-Switch

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

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

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, MXL

## show accounting

Display the active accounting sessions for each online user.

**Syntax** `show accounting`

**Defaults** none

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**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
  Task ID 1, EXEC Accounting record, 00:00:39 Elapsed, service=shell
Active accounted actions on tty3, User admin Priv 1
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed, service=shell
Dell#
```

## Related Commands

[aaa accounting](#) — enables AAA Accounting and creates a record for monitoring the accounting function.

# Authentication and Password Commands

This section contains the commands that control the management access to the system.

## 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

<b>default</b>	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> .
<b><i>method-list-name</i></b>	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.
<b><i>method</i></b>	Enter one of the following methods: <ul style="list-style-type: none"><li>• <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode.</li><li>• <code>line</code>: use the password the <code>password</code> command defines in LINE mode.</li><li>• <code>none</code>: no authentication.</li><li>• <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command.</li><li>• <code>tacacs+</code>: use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.</li></ul>
<b><i>... method2</i></b>	(OPTIONAL) In the event of a “no response” from the first method, Dell Networking Operating System (OS) applies the next configured method.

**Defaults** Use the `enable password`.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

## Usage Information

By default, the `Enable password` is used. If you configure `aaa authentication enable default`, Dell Networking Operating System (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 Operating System



(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.
- [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.

<b>Parameters</b>	<b><i>method-list-name</i></b>	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.
	<b>default</b>	Enter the keyword <code>default</code> to specify that the method list specified is the default method for all terminal lines.
	<b><i>method</i></b>	Enter one of the following methods: <ul style="list-style-type: none"> <li>• <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode.</li> <li>• <code>line</code>: use the password the <code>password</code> command defines in LINE mode.</li> <li>• <code>none</code>: no authentication.</li> <li>• <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command.</li> <li>• <code>tacacs+</code>: use the TACACS+ servers configured with the <code>tacacs-server host</code> command.</li> </ul>
	<b><i>... method4</i></b>	(OPTIONAL) Enter up to four additional methods. In the event of a "no response" from the first method, Dell Networking Operating System (OS) applies the next configured method (up to four configured methods).

**Defaults** Not configured (that is, no authentication is performed).

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.11(0.0)</b>	Included a prompt to force the users to re-authenticate, when re-authentication is enabled.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** By default, the locally configured username password is used. If you configure `aaa authentication login default`, Dell Networking Operating System (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 Operating System (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 Operating System (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 Operating System (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.

[radius-server host](#) — specifies a RADIUS server host.

[tacacs-server host](#) — specifies a TACACS+ server host.

## authorization

Apply an authorization method list to terminal lines.

**Syntax** `authorization {exec | commands {level | role role-name} method-list`

**Parameters**

<b>exec</b>	Enter the keyword <code>exec</code> to apply an EXEC level accounting method list.
<b>commands {level   role role-name}</b>	Enter the keywords <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. <code>role</code> method is supported only on Full-Switch mode.
<b>method-list</b>	Enter a method list that you defined using the <code>aaa accounting exec</code> or <code>aaa accounting</code> commands.

**Defaults** none

**Command Modes** LINE

**Supported Modes** All Modes.

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the support for roles on the MXL 10/40GbE Switch.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### 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.

<b>Parameters</b>	<b>commands <i>level</i></b>	Enter the keyword <code>commands</code> then the command privilege level for command level authorization.
	<b>role <i>role-name</i></b>	Enter the keyword <code>role</code> then the role name. <code>role</code> method is supported only on Full-Switch mode.
	<b><i>name</i></b>	Define a name for the list of authorization methods.
	<b>default</b>	Define the default list of authorization methods.
	<b>local</b>	Use the authorization parameters on the system to perform authorization.
	<b>tacacs+</b>	Use the TACACS+ protocol to perform authorization.
	<b>none</b>	Enter the keyword <code>none</code> to apply no authorization.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** All Modes.

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the support for roles on the MXL 10/40GbE Switch .
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

<b>Parameters</b>	<b><i>name</i></b>	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).
	<b>inherit <i>existing-role-name</i></b>	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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.7(0.0)</b>	Introduced on the S6000-ON.
	<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

**Usage Information** By default, access to commands are determined by the user's role (if defined) or by the user's privilege level. If the `aaa authorization role-only` command is enabled, then only the user's role is used.

Before you enable role-based only AAA authorization:

1. Locally define a system administrator user role. This will give you access to login with full permissions even if network connectivity to remote authentication servers is not available.

2. Configure login authentication on the console. This ensures that all users are properly identified through authentication no matter the access point
3. Specify an authentication method (RADIUS, TACACS+, or Local).
4. Specify authorization method (RADIUS, TACACS+ or Local).
5. Verify the configuration has been applied to the console or VTY line.

**Related Commands** login authentication, password, radius-server host, tacacs-server host

## aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

**Syntax** `aaa authorization config-commands`  
 Disable authorization checking for CONFIGURATION level commands using the `no aaa authorization config-commands` command.

**Defaults** Enabled when you configure `aaa authorization commands` command.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes.

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. To enable only EXEC-level command checking, use the command `no aaa authorization config-commands role` method is supported only on Full-Switch mode.

## aaa authorization exec

Set parameters that restrict (or permit) a user's access to EXEC-level commands.

**Syntax** `aaa authorization exec {name | default} {local || tacacs+ || if-authenticated || none}`  
 To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

Parameters	Parameter	Description
	<b>name</b>	Define a name for the list of authorization methods.
	<b>default</b>	Define the default list of authorization methods.
	<b>local</b>	Use the authorization parameters on the system to perform authorization.
	<b>tacacs+</b>	Use the TACACS+ protocol to perform authorization.
	<b>none</b>	Enter the keyword <code>none</code> to apply no authorization.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## aaa reauthenticate enable

Enable re-authentication of user whenever there is a change in the authenticators.

<b>Syntax</b>	<code>aaa reauthenticate enable</code> To disable the re-authentication option, use the <code>no aaa reauthenticate enable</code> command.
<b>Defaults</b>	Disabled
<b>Command Modes</b>	CONFIGURATION
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .

Version	Description
9.11(0.0)	Introduced this command.

**Usage Information** When an operating system enables to change the user authenticators, the users might access resources and perform tasks that they do not have authorization.

Once re-authentication is enabled, Dell EMC Networking OS prompts the users to re-authenticate whenever there is a change in authenticators.

The change in authentication happens when:

- Add or remove an authentication server (RADIUS/TACACS+)
- Modify an AAA authentication/authorization list
- Change to role-only (RBAC) mode

The re-authentication is also applicable for authenticated 802.1x devices. When there is a change in the authentication servers, the supplicants connected to all the ports are forced to re-authenticate.

### Example

```
DellEMC(config)#aaa reauthenticate enable
```

```
DellEMC(config)#aaa authentication login vty_auth_list radius
Force all logged-in users to re-authenticate (y/n)?
```

```
DellEMC(config)#radius-server host 192.100.0.12
Force all logged-in users to re-authenticate (y/n)?
```

## privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

<b>Syntax</b>	<code>privilege mode {level level command   reset command}</code> To delete access to a level and command, use the <code>no privilege mode level level command</code> command.
---------------	---

<b>Parameters</b>	<b>mode</b>	Enter one of the following keywords as the mode for which you are controlling access: <ul style="list-style-type: none"> <li>• <code>configure</code> for CONFIGURATION mode</li> <li>• <code>exec</code> for EXEC mode</li> <li>• <code>interface</code> for INTERFACE modes</li> <li>• <code>line</code> for LINE mode</li> </ul>
-------------------	-------------	---

- `route-map` for ROUTE-MAP mode
- `router` for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes

**level *level*** Enter the keyword `level` then a number for the access level. The range is from 0 to 15.

Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.

**reset** Enter the keyword `reset` to return the security level to the default setting.

**command** Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 *level*** Enter the keyword `level` then a number for the access level. The range is from 0 to 15.  
Level 1 is EXEC mode and Level 15 allows access to all CLI modes.

**Defaults** `level = 15`

**Command Modes** LINE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## banner exec

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

**Syntax** `banner exec c line c`  
To delete a banner, use the `no banner exec` command.

**Parameters** ***c*** Enter the keywords `banner exec`, then enter a character delineator, represented here by the letter `c`. Press **ENTER**.

**line** Enter a text string for your banner message ending the message with your delineator. In the following example, the delineator is a percent character (%); the banner message is “testing, testing”.

**Defaults** No banner is displayed.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

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

### Example

```
Dell(conf)#banner 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**

- [banner login](#) — sets a banner for login connections to the system.
- [exec-banner](#) — enables the display of a text string when you enter EXEC mode.
- [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*]

Parameters		
<b>keyboard-interactive</b>		Enter the keyword <code>keyboard-interactive</code> to require a carriage return (CR) to get the message banner prompt.
<b>c</b>		Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
<b>line</b>		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

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

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

### Example

```
Dell(conf)#banner login ?
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** [exec-banner](#)— 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*

**Parameters**

<b><i>c</i></b>	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
<b><i>line</i></b>	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

**Supported Modes** All Modes



<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	After entering the banner login command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When the user is connected to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After the user has logged in, the EXEC banner (if configured) displays.	
<b>Related Commands</b>	<a href="#">banner exec</a> — enables the display of a text string when you enter EXEC mode. <a href="#">banner login</a> — sets a banner to display after successful login to the system.	

## debug radius

View RADIUS transactions to assist with troubleshooting.

<b>Syntax</b>	<code>debug radius</code>
	To disable debugging of RADIUS, use the <code>no debug radius</code> command.
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	EXEC Privilege
<b>Supported Modes</b>	All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

## debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

<b>Syntax</b>	<code>debug tacacs+</code>
	To disable debugging of TACACS+, use the <code>no debug tacacs+</code> command.
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	EXEC Privilege
<b>Supported Modes</b>	All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

## exec-banner

Enable the display of a text string when the user enters EXEC mode.

**Syntax** `exec-banner`

To disable the banner on terminal lines, use the `no exec-banner` command.

**Defaults** **Enabled on all lines** (if configured, the banner appears).

**Command Modes** LINE

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** Optionally, use the `banner exec` command to create a text string that is displayed when you access EXEC mode. This command toggles that display.

**Related Commands** [banner exec](#)— configures a banner to display when entering EXEC mode.  
[line](#) — enables and configures console and virtual terminal lines to the system.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Parameters</b>	<b>level</b> <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.
	<b>encryption-type</b>	(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.
	<b>password</b>	Enter a text string, up to 32 characters long, as the clear text password.

**Defaults** No password is configured. *level* = **15**.

**Command Modes** CONFIGURATION


**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 (?) is not a supported character.

**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.

<b>Parameters</b>	<b>encryption-type</b>	(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.
	<b>password</b>	Enter a text string, up to 32 characters long, as the clear text password.

**Defaults** Not configured.

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Only Dell Networking Technical Support staff use this command.

## enable secret

Change the password for the `enable` command.

<b>Syntax</b>	<code>enable secret [level level] [encryption-type] password</code>	
	To delete a password, use the <code>no enable secret [encryption-type] password [level level]</code> command.	
<b>Parameters</b>	<b>level level</b>	(OPTIONAL) Enter the keyword <code>level</code> then a number as the level of access. The range is from 1 to 15.
	<b>encryption-type</b>	(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.
	<b>password</b>	Enter a text string, up to 32 characters long, as the clear text password.

**Defaults** No password is configured. `level = 15`.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch


Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 (?) is not a supported character.

**Related Commands**

[show running-config](#) — views the current configuration.

[privilege level \(CONFIGURATION mode\)](#) — controls access to the command modes within the switch.

## enable sha256-password

Configure SHA-256 based password for the `enable` command.

<b>Syntax</b>	<code>enable sha256-password [level level] [encryption-type] password</code>
---------------	--

To delete a password, use the `no enable sha256-password [encryption-type] password [level level]` command.

<b>Parameters</b>	<b>sha256-password</b>	Enter the keyword <code>sha256-password</code> then the <code>encryption-type</code> or the password.
	<b>level level</b>	(OPTIONAL) Enter the keyword <code>level</code> then a number as the level of access. The range is from 1 to 15.
	<b>encryption-type</b>	(OPTIONAL) Enter the number 8 or 0 as the encryption type. Enter 8 to enter the sha256-based hashed password.
	<b>password</b>	Enter a text string, up to 32 characters long, as the clear text password.

**Defaults** No password is configured. `level = 15`.

**Command Modes** CONFIGURATION

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

Version	Description
9.10(0.0)	Introduced on the MXL.

**Related Commands**

- [show running-config](#) — views the current configuration.
- [privilege level \(CONFIGURATION mode\)](#) — controls access to the command modes within the switch.

## login authentication

To designate the terminal lines, apply an authentication method list.

**Syntax** `login authentication {method-list-name | default}`

To use the local user/password database for login authentication, use the `no login authentication` command.

<b>Parameters</b>	<b>method-list-name</b>	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.
	<b>default</b>	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

**Supported Modes** All Modes

<b>Command History</b>	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	9.3(0.0)	Supported on the M I/O Aggregator.

**Usage Information** If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.

**Related Commands** [aaa authentication login](#) — selects the login authentication methods.

## password

Specify a password for users on terminal lines.

**Syntax** `password [encryption-type] password`

To delete a password, use the `no password password` command.

**Parameters**

**encryption-type** (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the password entered. The options are

- 0 is the default and means the password is not encrypted and stored as clear text.
- 7 means that the password is encrypted and hidden.

**password** Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

**Defaults** No password is configured.

**Command Modes** LINE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system prompts users for these passwords when the method for authentication or authorization used is "line".

**Related Commands**

- [enable password](#) — sets the password for the `enable` command.
- [login authentication](#) — configures an authentication method to log in to the switch.
- [service password-encryption](#) — encrypts all passwords configured in the system.
- [radius-server key](#) — configures a key for all RADIUS communications between the switch and the RADIUS host server.
- [tacacs-server key](#) — configures a key for communication between a TACACS+ server and client.
- [username](#) — establishes an authentication system based on user names.

## password-attributes

Configure the password attributes (strong password).

**Syntax** `password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]`

To return to the default, use the `no password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]` command.

**Parameters**

**min-length number** (OPTIONAL) Enter the keywords `min-length` then the number of characters. The range is from 0 to 32 characters.

**max-retry number** (OPTIONAL) Enter the keywords `max-retry` then the number of maximum password retries. The range is from 0 to 16.

**lockout-period minutes** (OPTIONAL) Enter the keyword `lockout-period` then the number of minutes. The range is from 1 to 1440 minutes. The default is 0 minutes and the lockout-period is not enabled. This parameter enhances the security of the switch by

locking out sessions on the Telnet or SSH sessions for which there has been a consecutive failed login attempts. The console is not locked out.

- character-restriction** (OPTIONAL) Enter the keywords `character-restriction` to indicate a character restriction for the password.
- upper *number*** (OPTIONAL) Enter the keyword `upper` then the upper number. The range is from 0 to 31.
- lower *number*** (OPTIONAL) Enter the keyword `lower` then the lower number. The range is from 0 to 31.
- numeric *number*** (OPTIONAL) Enter the keyword `numeric` then the numeric number. The range is from 0 to 31.
- special-char *number*** (OPTIONAL) Enter the keywords `special-char` then the number of special characters permitted. The range is from 0 to 31.

The following special characters are supported:

! " # % & ' ( ) ; < = > ? [ \ ] \* + , - . / : ^ \_ { | } ~ @ \$

- Defaults** none
- Command Modes** CONFIGURATION
- Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.6(0.0)	Introduced the special-characters on the MXL Switch.
	9.5(0.0)	Introduced the <code>lockout-period</code> option on the MXL 10/40GbE Switch.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

- Related Commands** [password](#) — specifies a password for users on terminal lines.


## service password-encryption

Encrypt all passwords configured in the system.

- Syntax** `service password-encryption`  
To store new passwords as clear text, use the `no service password-encryption` command.

- Defaults** Enabled.
- Command Modes** CONFIGURATION
- Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

- 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the support for roles on the MXL 10/40GbE Switch.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show user` command shown in the following example.

Field	Description
<b>(untitled)</b>	Indicates with an asterisk (*) which terminal line you are using.
<b>Line</b>	Displays the terminal lines currently in use.



Field	Description
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.

## secure-cli enable

Enable the secured CLI mode.

**Syntax** `secure-cli enable`

**Command Modes** CONFIGURATION

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

Version	Description
9.11(0.0)	Introduced this command.

**Usage Information** The secured CLI mode prevents the users from enhancing the permissions or promoting the privilege levels. After entering the command, save the running-configuration.

Once you save the running-configuration, the secured CLI mode is enabled. If you do not want to enter the secured mode, do not save the running-configuration.

Once saved, to disable the secured CLI mode, you need to manually edit the startup-configuration file and reboot the system.

## 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

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**8.3.16.1**

Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is "password" you can enter "p" and wait 29 seconds to enter the next letter.

## username

Establish an authentication system based on user names.

**Syntax**

```
username name [access-class access-list-name] [nopassword | {password | secret | sha256-password} [encryption-type] password] [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**

<b><i>name</i></b>	Enter a text string for the name of the user up to 63 characters.
<b><i>access-class</i></b> <b><i>access-list-name</i></b>	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).
<b><i>nopassword</i></b>	Enter the keyword <code>nopassword</code> to specify that the user should not enter a password.
<b><i>password</i></b>	Enter the keyword <code>password</code> then the <code>encryption-type</code> or the password.
<b><i>secret</i></b>	Enter the keyword <code>secret</code> then the <code>encryption-type</code> or the password.
<b><i>encryption-type</i></b>	Enter an encryption type for the password that you enter. <ul style="list-style-type: none"><li>• 0 directs the system to store the password as clear text. It is the default encryption type when using the <code>password</code> option.</li><li>• 8 to indicate that a password encrypted using a sha256 hashing algorithm follows. This encryption type is available with the <code>sha256-password</code> option only, and is the default encryption type for this option.</li><li>• 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.</li><li>• 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.</li></ul>
<b><i>password</i></b>	Enter a string up to 32 characters long.
<b><i>privilege level</i></b>	Enter the keyword <code>privilege</code> then a number from zero (0) to 15.
<b><i>role role-name</i></b>	Enter the keyword <code>role</code> followed by the role name to associate with that user ID.
<b><i>secret</i></b>	Enter the keyword <code>secret</code> then the encryption type.
<b><i>sha256-password</i></b>	Enter the keyword <code>sha256-password</code> then the <code>encryption-type</code> or the password.

**Defaults**

The default encryption type for `password` option is **0**. The default encryption type for `secret` option is **5**. The default encryption type for `sha256-password` option is **8**. The default value of `privilege level` is **1**.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th>Version</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>9.10(0.0)</b></td> <td>Added support for the <code>sha256-password</code> option.</td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.5(0.0)</b></td> <td>Introduced the support for roles on the MXL 10/40GbE Switch.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	<b>9.10(0.0)</b>	Added support for the <code>sha256-password</code> option.	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.5(0.0)</b>	Introduced the support for roles on the MXL 10/40GbE Switch.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description										
<b>9.10(0.0)</b>	Added support for the <code>sha256-password</code> option.										
<b>9.9(0.0)</b>	Introduced on the FN IOM.										
<b>9.5(0.0)</b>	Introduced the support for roles on the MXL 10/40GbE Switch.										
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.										
<b>Usage Information</b>	To view the defined user names, use the <code>show running-config user</code> command.										
<b>Related Commands</b>	<p><code>password</code> — specifies a password for users on terminal lines.</p> <p><code>show running-config</code> — views the current configuration.</p>										

## RADIUS Commands

The following RADIUS commands are supported by Dell Networking Operating System (OS).

### client

Configures trusted DAC clients.

<b>Syntax</b>	<pre>client {ipv4-addr   ipv6-addr   hostname} [vrf vrf-name] [key [encryption-type] key]</pre> <p>To undo the DAC client configuration, enter the <code>no client host</code> command.</p>														
<b>Defaults</b>	If VRF is not configured, default VRF is considered.														
<b>Parameters</b>	<table border="0"> <tr> <td><b>ipv4-addr</b></td> <td>Enter the keyword <code>ipv4-addr</code> to specify the IPv4 address of the DAC.</td> </tr> <tr> <td><b>ipv6-addr</b></td> <td>Enter the keyword <code>ipv6-addr</code> to specify the IPv6 address of the DAC.</td> </tr> <tr> <td><b>hostname</b></td> <td>Enter the keyword <code>hostname</code> to enter the name of the host.</td> </tr> <tr> <td><b>vrf vrf-name</b></td> <td>Enter the keyword <code>vrf</code> followed by the name of the VRF to associate a VRF with the client.</td> </tr> <tr> <td><b>key</b></td> <td>(Optional) Enter the keyword <code>key</code> to specify an encryption key.</td> </tr> <tr> <td><b>encryption-type</b></td> <td>(Optional) Enter either 0 or 7 as the encryption type for the specified key. The options are: <ul style="list-style-type: none"> <li>• 0 – implies that the key is not encrypted and is stored as clear text.</li> <li>• 7 – implies that the key is encrypted and hidden.</li> </ul> </td> </tr> <tr> <td><b>key</b></td> <td>Enter a string that is the key to be exchanged between the switch and the dynamic authorization client. The key can be up to 42 characters long.</td> </tr> </table>	<b>ipv4-addr</b>	Enter the keyword <code>ipv4-addr</code> to specify the IPv4 address of the DAC.	<b>ipv6-addr</b>	Enter the keyword <code>ipv6-addr</code> to specify the IPv6 address of the DAC.	<b>hostname</b>	Enter the keyword <code>hostname</code> to enter the name of the host.	<b>vrf vrf-name</b>	Enter the keyword <code>vrf</code> followed by the name of the VRF to associate a VRF with the client.	<b>key</b>	(Optional) Enter the keyword <code>key</code> to specify an encryption key.	<b>encryption-type</b>	(Optional) Enter either 0 or 7 as the encryption type for the specified key. The options are: <ul style="list-style-type: none"> <li>• 0 – implies that the key is not encrypted and is stored as clear text.</li> <li>• 7 – implies that the key is encrypted and hidden.</li> </ul>	<b>key</b>	Enter a string that is the key to be exchanged between the switch and the dynamic authorization client. The key can be up to 42 characters long.
<b>ipv4-addr</b>	Enter the keyword <code>ipv4-addr</code> to specify the IPv4 address of the DAC.														
<b>ipv6-addr</b>	Enter the keyword <code>ipv6-addr</code> to specify the IPv6 address of the DAC.														
<b>hostname</b>	Enter the keyword <code>hostname</code> to enter the name of the host.														
<b>vrf vrf-name</b>	Enter the keyword <code>vrf</code> followed by the name of the VRF to associate a VRF with the client.														
<b>key</b>	(Optional) Enter the keyword <code>key</code> to specify an encryption key.														
<b>encryption-type</b>	(Optional) Enter either 0 or 7 as the encryption type for the specified key. The options are: <ul style="list-style-type: none"> <li>• 0 – implies that the key is not encrypted and is stored as clear text.</li> <li>• 7 – implies that the key is encrypted and hidden.</li> </ul>														
<b>key</b>	Enter a string that is the key to be exchanged between the switch and the dynamic authorization client. The key can be up to 42 characters long.														
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• CONF-DYNAMIC-AUTH</li> </ul>														
<b>Usage Information</b>	<ul style="list-style-type: none"> <li>• It is possible to configure more than one dynamic authorization clients Duplicate (<code>ipv4-addr</code> or <code>ipv6-addr</code> or <code>host-name</code>) configurations are not allowed.</li> </ul>														
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell EMC Networking OS version history for this command.</p> <table border="0"> <thead> <tr> <th>Version</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>9.14(1.0)</b></td> <td>Introduced on the S4810 and S4820T.</td> </tr> </tbody> </table>	Version	Description	<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.										
Version	Description														
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.														

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FM-IOM, and MXL.

## client-key

Configures global shared key for the trusted DAC clients.

<b>Syntax</b>	<code>client-key [encryption-type] key</code> To remove the shared key configuration, enter the <code>no client-key</code> command.
<b>Defaults</b>	None.
<b>Parameters</b>	<p><b>encryption-type:</b> (OPTIONAL) Enter either 0 or 7 as the encryption type for the key entered. The options are:</p> <ul style="list-style-type: none"> <li>0 — is the default and means the key is not encrypted and stored as clear text.</li> <li>7 — means that the key is encrypted and hidden.</li> </ul> <p><b>key</b> Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.</p>
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>CONF-DYNAMIC-AUTH</li> </ul>
<b>Usage Information</b>	<ul style="list-style-type: none"> <li>Configure global shared key applicable for DA clients. If client configuration has shared key configured, that will take precedence.</li> </ul>
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell EMC Networking OS version history for this command.</p>

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## coa-bounce-port

Configure NAS to allow or reject the port bounce RADIUS messages from DAC.

<b>Syntax</b>	<code>coa-bounce-port</code> To remove the port bounce configuration, enter the <code>no coa-bounce-port</code> command.
<b>Defaults</b>	Enabled.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>CONF-DYNAMIC-AUTH</li> </ul>
<b>Usage Information</b>	<ul style="list-style-type: none"> <li>Configure <code>no coa-bounce-port</code> to drop radius CoA port-bounce requests from the DAC.</li> </ul>
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell EMC Networking OS version history for this command.</p>
<b>Version</b>	<b>Description</b>
9.14(1.0)	Introduced on the S4810 and S4820T.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## coa-disable-port

Configure NAS to reject disable-port requests from DAC.

**Syntax** `coa-disable-port`  
To undo this configuration, enter the `no coa-disable-port` command.

**Defaults** Enabled.

**Command Modes** • CONF-DYNAMIC-AUTH

**Usage Information** • Configure `no coa-disable-port` DAS to drop radius CoA disable-port requests from DAC.

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

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

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## coa-reauthenticate

Configure NAS to re-authenticate dot1x user session requests from DAC.

**Syntax** `coa-reauthenticate`  
To allow or reject re-authentication requests, enter the `no coa-reauthenticate` command.

**Defaults** Enabled.

**Command Modes** • CONF-DYNAMIC-AUTH

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

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

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## debug radius

View RADIUS transactions to assist with troubleshooting.

**Syntax** `debug radius`

To disable debugging of RADIUS, use the `no debug radius` command.

- Defaults** Disabled.
- Command Modes** EXEC Privilege
- Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## da-rsp-timeout

Configure timeout value for the back end task to respond to DAC requests.

- Syntax** `da-rsp-timeout minutes`
- To undo the configuration, enter the `no da-rsp-timeout` command.

**Defaults** 10 Minutes.

**Parameters** *minutes* Enter the time out value.

- Command Modes**
- CONF-DYNAMIC-AUTH
- Usage Information**
- Time for DAS to wait before the back end response is received.

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

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## disconnect-user

Configure NAS to allow or reject DM requests corresponding to AAA users-sessions coming from the DAC.

- Syntax** `disconnect-user`
- To undo this configuration, enter the `no disconnect-user` command.

**Defaults** Enabled.

**Command Modes**

- CONF-DYNAMIC-AUTH

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

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## dynamic-auth-enable

Configure NAS to receive and process dynamic authorization messages.

<b>Syntax</b>	<code>dynamic-auth-enable</code>  To stop NAS from receiving and processing dynamic authorization messages, use the <code>no dynamic-auth-enable</code> command.
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>CONF-DYNAMIC-AUTH</li> </ul>
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell EMC Networking OS version history for this command.</p>

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.13(0.0)	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

<b>Usage Information</b>	If this configuration is not enabled, then dynamic authorization messages are not handled by the NAS.
--------------------------	---

## ip radius source-interface

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

<b>Syntax</b>	<code>ip radius source-interface interface</code>  To delete a source interface, use the <code>no ip radius source-interface</code> command.						
<b>Parameters</b>	<p><b><i>interface</i></b> Enter the following keywords and slot/port or number information:</p> <ul style="list-style-type: none"> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>For a ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	All Modes						
<b>Command History</b>	<table> <thead> <tr> <th>Version</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>9.9(0.0)</td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td>9.4(0.0)</td> <td>Supported on the FN I/O Aggregator.</td> </tr> </tbody> </table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	9.4(0.0)	Supported on the FN I/O Aggregator.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
9.4(0.0)	Supported on the FN I/O Aggregator.						

## port

Configures NAS port number to accept CoA or DM requests.

**Syntax** `port port-number`  
To remove the NAS port configuration, enter the `no port` command.

**Defaults** 3799

**Parameters** *port-number* Enter the NAS port number to accept CoA and DM requests. The range is from 1 to 65535.

- Command Modes**
- CONF-DYNAMIC-AUTH
- Usage Information**
- Optionally specify dynamic authorization port number. Default port is 3799.

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

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## radius dynamic-auth

Enters a new sub-mode, RADIUS-DYNAMIC-AUTH, which enables you to modify dynamic authorization settings.

**Syntax** `radius dynamic-auth`  
To remove the dynamic authorization method for RADIUS users, enter the `no radius dynamic-auth` command.

**Defaults** Disabled.

**Command Modes**

- CONFIGURATION

**Usage Information**

- All dynamic authorization commands are configured by entering this mode.

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

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

**Syntax** `radius-server deadtime seconds`



To disable this function or return to the default value, use the `no radius-server deadtime` command.

**Parameters**            **seconds**            Enter a number of seconds during which non-responsive RADIUS servers are skipped. The range is from 0 to 2147483647 seconds. The default is **0 seconds**.

**Defaults**            **0 seconds**

**Command Modes**    CONFIGURATION

**Supported Modes**   All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

## 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**

<b>hostname</b>	Enter the name of the RADIUS server host.
<b>ipv4-address   ipv6-address</b>	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X::X) of the RADIUS server host.
<b>auth-port port-number</b>	(OPTIONAL) Enter the keywords <code>auth-port</code> then a number as the port number. The range is from zero (0) to 65535. The default port-number is <b>1812</b> .
<b>retransmit retries</b>	(OPTIONAL) Enter the keyword <code>retransmit</code> then a number as the number of attempts. This parameter overwrites the <code>radius-server retransmit</code> command. The range is from zero (0) to 100. The default is <b>3 attempts</b> .
<b>timeout seconds</b>	(OPTIONAL) Enter the keyword <code>timeout</code> then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the <code>radius-server timeout</code> command. The range is from 0 to 1000. The default is <b>5 seconds</b> .
<b>key [encryption-type] key</b>	(OPTIONAL) Enter the keyword <code>key</code> 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: <ul style="list-style-type: none"><li>• 0 is the default and means the password is not encrypted and stored as clear text.</li><li>• 7 means that the password is encrypted and hidden.</li></ul> Configure this parameter last because leading spaces are ignored.

**Defaults**            Not configured.

**Command Modes**    CONFIGURATION

**Supported Modes**   All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
9.3(0.0)	Supported on the M I/O Aggregator.

#### Usage Information

To configure any number of RADIUS server hosts for each server host that is configured, use this command. Dell Networking Operating System (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.

#### Related Commands

[login authentication](#) — sets the database to be checked when a user logs in.

[radius-server retransmit](#) — sets the number of times the RADIUS server attempts to send information.

[radius-server timeout](#) — sets the time interval before the RADIUS server times out.

## radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

**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

**Supported Modes** All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.3(0.0)	Supported on the M I/O Aggregator.

#### 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.

<b>Parameters</b>	<b><i>retries</i></b>	Enter a number of attempts that Dell Networking Operating System (OS) tries to locate a RADIUS server. The range is from zero (0) to 100. The default is <b>3 retries</b> .
<b>Defaults</b>	<b>3 retries</b>	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.
<b>Related Commands</b>	<a href="#">radius-server host</a>	— 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 .

<b>Syntax</b>	<code>radius-server timeout <i>seconds</i></code>	
	To return to the default value, use the <code>no radius-server timeout</code> command.	
<b>Parameters</b>	<b><i>seconds</i></b>	Enter the number of seconds between an unsuccessful attempt and the radius-server timeout times out. The range is from zero (0) to 1000 seconds. The default is <b>5 seconds</b> .
<b>Defaults</b>	<b>5 seconds</b>	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.
<b>Related Commands</b>	<a href="#">radius-server host</a>	— configures a RADIUS host.

## role

Changes command permissions for roles.

<b>Syntax</b>	<code>role mode { { { <i>addrole</i>   <i>deleterole</i> } <i>role-name</i> }   reset } <i>command</i></code>	
	To delete access to a command, use the <code>no role <i>mode</i> <i>role-name</i></code>	
<b>Parameters</b>	<b><i>mode</i></b>	Enter one of the following keywords as the mode for which you are controlling access:  configure for CONFIGURATION mode

exec for EXEC mode  
 interface for INTERFACE modes  
 line for LINE mode  
 route-map for Route-map mode  
 router for Router mode

**addrole** Enter the keyword `addrole` to add permission to the command. You cannot add or delete rights for the `sysadmin` role.

**deleterole** Enter the keyword `deleterole` to remove access to the command. You cannot add or delete rights for the `sysadmin` role.

**role-name** Enter a text string for the name of the user role up to 63 characters. These are 3 system defined roles you can modify: `secadmin`, `netadmin`, and `netoperator`.

**reset** Enter the keyword `reset` to reset all roles back to default for that command.

**command** Enter the command's keywords to assign the command to a certain access level. You can enter one or more keywords.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced on the MXL.

**Related Commands** `userrole`

## rate-limit

Configure NAS to allow or reject RADIUS dynamic authorization (DA) packets based on the configurable rate limit value.

**Syntax** `rate-limit packets per minute`  
 To undo the configuration, enter the `no rate-limit` command.

**Defaults** 30 packets per minute.

**Parameters** **packet per minute** Enter the number of packets that you want processed per minute. The range is between 10 to 60 packets per minute.

**Command Modes** • CONF-DYNAMIC-AUTH

**Usage Information** • Packets are dropped after number of packets reaches the configured rate-limit.

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

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## replay-protection-window

Configure replay protection window period to drop the duplicate packets.

<b>Syntax</b>	<code>replay-protection-window minutes</code> To undo the configuration, enter the <code>no replay-protection-window</code> command.
<b>Defaults</b>	5 Minutes.
<b>Parameters</b>	<b>minutes</b> Enter the number of minutes to drop the packets. The range is from 1 to 10 minutes.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>CONF-DYNAMIC-AUTH</li></ul>
<b>Usage Information</b>	<ul style="list-style-type: none"><li>Duplicate packets are dropped within replay-protection-window period if packet has same source IP address, source UDP port and identifier.</li></ul>
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## terminate-session

Configure NAS to reject dot1x terminate-session requests from DAC.

<b>Syntax</b>	<code>terminate-session</code> To drop the DM terminate-session requests from DAC, enter the <code>no terminate-session</code> command.
<b>Defaults</b>	Enabled.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>CONF-DYNAMIC-AUTH</li></ul>
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .

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

Version	Description
<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on the C9010, S3100, S3048-ON, S4048T-ON, S4048-ON, S5000, S6010-ON, S6000-ON, S6100-ON, S6000, Z9100-ON, Z9500, FN-IOM, and MXL.

## show privilege

View your access level.

<b>Syntax</b>	<code>show privilege</code>
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>
<b>Supported Modes</b>	All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

#### Example

```
Dell#show privilege
Current privilege level is 15
Dell#
```

## Suppressing AAA Accounting for Null Username Sessions

When you activate AAA accounting, the Dell Networking OS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL.

An example of this is a user who comes in on a line where the AAA authentication `login method-list none` command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command.

- Prevent accounting records from being generated for users whose username string is NULL.

```
CONFIGURATION mode
aaa accounting suppress null-username
```

## TACACS+ Commands

Dell Networking OS supports TACACS+ as an alternate method for login authentication.

### TACACS+ Accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

**Syntax** `aaa accounting {system | exec | commands level} {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

<b><i>system</i></b>	Enter the keyword <i>system</i> to send accounting information of any other AAA configuration.
<b><i>exec</i></b>	Enter the keyword <i>exec</i> to send accounting information when a user has logged in to EXEC mode.
<b><i>commands level</i></b>	Enter the keyword <i>command</i> then a privilege level for accounting of commands executed at that privilege level.
<b><i>name   default</i></b>	Enter one of the following: <ul style="list-style-type: none"> <li>For <i>name</i>, enter a user-defined name of a list of accounting methods.</li> <li>For <i>default</i>, the default accounting methods used.</li> </ul>
<b><i>start-stop</i></b>	Enter the keywords <i>start-stop</i> to send a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
<b><i>wait-start</i></b>	Enter the keywords <i>wait-start</i> to ensure that the TACACS+ security server acknowledges the start notice before granting the user's process request.

**stop-only** Enter the keywords `stop-only` to instruct the TACACS+ security server to send a "stop record accounting" notice at the end of the requested user process.

**tacacs+** Enter the keyword `tacacs+` to use TACACS+ data for accounting.

Dell Networking OS currently only supports TACACS+ accounting.

**Defaults** None

**Command Modes** CONFIGURATION

**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`.

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Supported on the FN I/O Agregator and M I/O Agregator.

#### Example

```
Dell(config)# aaa accounting exec default start-stop tacacs+
Dell(config)# aaa accounting command 15 default start-stop tacacs+
Dell(config)#
```

Related Commands	Command	Description
	<b>enable password</b>	changes the password for the enable command.
	<b>login authentication</b>	enables AAA login authentication on the terminal lines.
	<b>password</b>	creates a password.
	<b>tacacs-server host</b>	specifies a TACACS+ server host.

## debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

**Syntax** `debug tacacs+`  
To disable debugging of TACACS+, use the `no debug tacacs+` command.

**Defaults** Disabled.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

<b>Parameters</b>	<b><i>interface</i></b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li> </ul>
-------------------	-------------------------	---

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

## tacacs-server host

Specify a TACACS+ host.

**Syntax** `tacacs-server host {hostname | ipv4-address | ipv6-address} [port number] [timeout seconds] [key key]`

<b>Parameters</b>	<b><i>hostname</i></b>	Enter the name of the TACACS+ server host.
	<b><i>ipv4-address   ipv6-address</i></b>	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X::X) of the TACACS+ server host.
	<b><i>port number</i></b>	(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 <b>49</b> .
	<b><i>timeout seconds</i></b>	(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 <b>10 seconds</b> .
	<b><i>key key</i></b>	(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

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** To list multiple TACACS+ servers to be used by the `aaa authentication login` command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the `port`, `timeout` and `key` optional parameters. If you do not configure a key, the key assigned in the `tacacs-server key` command is used.

**Related Commands** [aaa authentication login](#) — specifies the login authentication method.  
[tacacs-server key](#) — configures a TACACS+ key for the TACACS server.



## tacacs-server key

Configure a key for communication between a TACACS+ server and a client.

**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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** The key configured with this command must match the key configured on the TACACS+ daemon.

## 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**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.

# SSH Server and SCP Commands

The Dell Networking OS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.


## crypto key generate

Generates keys for the SSH server.

<b>Syntax</b>	<code>crypto key generate {rsa   rsa1}</code>	
<b>Parameters</b>	<b>rsa</b>	Enter the keyword <code>rsa</code> then the key size to generate a SSHv2 RSA host keys. The range is from 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is <b>1024</b> .
	<b>rsa1</b>	Enter the keyword <code>rsa1</code> then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048. The default is <b>1024</b> .
<b>Defaults</b>	Key size <b>1024</b> ; if you enable FIPS mode, the key size is <b>2048</b> .	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The host keys are required for key-exchange by the SSH server. If the keys are not found when you enable the server (`ip ssh server enable`), the keys are automatically generated.

This command requires user interaction and generates a prompt prior to overwriting any existing host keys.

 **NOTE:** Only a user with superuser permissions should generate host-keys.

### Example

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

**Related Commands** [ip ssh server](#) — enables the SSH server.  
[show crypto](#) — displays the SSH host public keys.

## 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.

<b>Defaults</b>	Disabled on both client and server.	
<b>Command Modes</b>	EXEC	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>ip scp topdir <i>directory</i></code>	
	To return to the default setting, use the <code>no ip scp topdir</code> command.	
<b>Parameters</b>	<b><i>directory</i></b>	Enter a directory name.
<b>Defaults</b>	The internal flash ( <code>flash:</code> ) is the default directory.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	To configure the switch as an SCP server, use the <code>ip ssh server</code> command.	
<b>Related Commands</b>	<a href="#">ip ssh server</a> — 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.

<b>Syntax</b>	<code>ip ssh authentication-retries <i>1-10</i></code>	
<b>Parameters</b>	<b><i>1-10</i></b>	Enter the number of maximum retries to authenticate a user. The range is from 1 to 10. The default is <b>3</b> .
<b>Defaults</b>	<b>3</b>	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 cipher

Configure the list of ciphers supported on both SSH client and SCP.

**Syntax** `ip ssh cipher cipher-list`

**Parameters** **cipher cipher-list** Enter the keyword `cipher` and then a space-delimited list of ciphers that the SSH client supports. The following ciphers are available.

- `aes256-ctr`
- `aes256-cbc`
- `aes192-ctr`
- `aes192-cbc`
- `aes128-ctr`
- `aes128-cbc`
- `3des-cbc`

**Defaults** The default list of ciphers is in the order as shown below:

- `aes256-ctr`
- `aes256-cbc`
- `aes192-ctr`
- `aes192-cbc`
- `aes128-ctr`
- `aes128-cbc`
- `3des-cbc`

**Command Modes** CONFIGURATION

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

Version	Description
<b>9.10(0.0)</b>	Introduced on the S6100-ON, S6000, S6000-ON, S5000, S4810, S4820T, S3048-ON, S4048-ON, MXL, C9010, S3100 series, and Z9100-ON.

**Usage Information**

- You can select one or more ciphers from the list.
- The default list of supported ciphers is same irrespective of whether FIPS mode is enabled or disabled.
- Client-supported cipher list gets preference over the server-supported cipher list in selecting the cipher for the SSH session.
- When the `cipher (-c)` option is used with the SSH CLI, it overrides the configured or default cipher list.
- When FIPS is enabled or disabled, the client ciphers get default configuration.

## ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

**Syntax** `ip ssh hostbased-authentication enable`  
To disable hostbased-authentication for SSHv2 server, use the `no ip ssh hostbased-authentication enable` command.

**Parameters** **enable** Enter the keyword `enable` to enable hostbased-authentication for SSHv2 server.

**Defaults** Disabled.


**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

The server-generated key is used for SSHv1 key-exchange.

## ip ssh mac

Configure the list of MAC algorithms supported on both SSH client and SCP.

### Syntax

```
ip ssh mac mac-list
```

### Parameters

#### mac mac-list

Enter the keyword `mac` then a space-delimited list of message authentication code (MAC) algorithms supported by the SSH client. The following MAC algorithms are available.

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

### Defaults

The default list of MAC algorithm is in the order as shown below:

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

**Command Modes** CONFIGURATION

### Command History

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

#### Version

#### Description

##### 9.10(0.0)

Introduced on the S6100-ON, S6000, S6000-ON, S5000, S4810, S4820T, S3048-ON, S4048-ON, MXL, C9010, S3100 series, and Z9100-ON.

### Usage Information

- You can select one or more MAC algorithms from the list.
- Client-supported MAC list gets preference over the server-supported MAC list in selecting the MAC algorithm for the SSH session.
- When the `MAC (-m)` option is used with the SSH CLI, it overrides the configured or default MAC list.
- When FIPS is enabled or disabled, the client MACs get default configuration.


## ip ssh password-authentication

Enable password authentication for the SSH server.

<b>Syntax</b>	<code>ip ssh password-authentication enable</code> To disable password-authentication, use the <code>no ip ssh password-authentication enable</code> command.						
<b>Parameters</b>	<b>enable</b> Enter the keyword <code>enable</code> to enable password-authentication for the SSH server.						
<b>Defaults</b>	Enabled						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.						

## ip ssh rhostsfile

Specify the rhost file used for host-based authorization.

<b>Syntax</b>	<code>ip ssh rhostsfile {WORD}</code>						
<b>Parameters</b>	<b>WORD</b> Enter the rhost file name for the host-based authentication.						
<b>Defaults</b>	none						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Example</b>	<pre>Dell#conf Dell(conf)# ip ssh rhostsfile flash://shosts Dell(conf)#</pre>						
<b>Usage Information</b>	<p>This command specifies the rhost file used for host-based authentication. This <code>creates/</code> file overwrites the <code>flash:/ADMIN_DIR/ssh/shosts</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.</p> <p>This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.</p> <p> <b>NOTE:</b> For <code>rhostfile</code> and <code>pub-key-file</code>, the administrator must FTP the file to the switch.</p>						

## 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.

<b>Syntax</b>	<code>ip ssh rekey [time rekey-interval] [volume rekey-limit]</code> To reset to the default, use <code>no ip ssh rekey [time rekey-interval] [volume rekey-limit]</code> command.				
<b>Parameters</b>	<table><tr><td><b>time minutes</b></td><td>Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes</td></tr><tr><td><b>volume rekey-limit</b></td><td>Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b></td></tr></table>	<b>time minutes</b>	Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes	<b>volume rekey-limit</b>	Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b>
<b>time minutes</b>	Enter the keywords <code>time</code> then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is <b>60</b> minutes				
<b>volume rekey-limit</b>	Enter the keywords <b>volume</b> then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is <b>1024 megabytes</b>				
<b>Defaults</b>	The default time is <b>60</b> minutes. The default volume is <b>1024</b> megabytes.				
<b>Command Modes</b>	CONFIGURATION mode				
<b>Supported Modes</b>	Full-Switch				
<b>Command History</b>	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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON.
<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, MXL

## ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

<b>Syntax</b>	<code>ip ssh rsa-authentication enable</code> To disable RSA authentication, use the <code>no ip ssh rsa-authentication enable</code> command.						
<b>Parameters</b>	<table><tr><td><b>enable</b></td><td>Enter the keyword <code>enable</code> to enable RSA authentication for the SSHv2 server.</td></tr></table>	<b>enable</b>	Enter the keyword <code>enable</code> to enable RSA authentication for the SSHv2 server.				
<b>enable</b>	Enter the keyword <code>enable</code> to enable RSA authentication for the SSHv2 server.						
<b>Defaults</b>	Disabled.						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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 ( <code>ip ssh rsa-authentication my-authorized-keys device://filename</code> command).						
<b>Related Commands</b>	<a href="#">ip ssh rsa-authentication (EXEC)</a> — adds keys for RSA authentication.						



## ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

**Syntax** `ip ssh rsa-authentication {my-authorized-keys WORD}`  
To delete the authorized keys, use the `no ip ssh rsa-authentication {my-authorized-keys}` command.

**Parameters**

<b>my-authorized-keys <i>WORD</i></b>	Enter the keywords <code>my-authorized-keys</code> then the filename of the RSA authorized-keys.
---------------------------------------	--


**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you want to log in without being prompted for a password, log in through RSA authentication. To do that, first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file: `flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).

 **NOTE:** The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/authorized-keys-username` file.

**Related Commands**

- [show ip ssh rsa-authentication](#) — displays the RSA authorized keys.
- [ip ssh rsa-authentication \(Config\)](#) — enables RSA authentication.

## ip ssh server

Configure an SSH server.

**Syntax** `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}` command.

**Parameters**

<b>enable</b>	Enter the keyword <code>enable</code> to start the SSH server.
<b>ciphers <i>cipher-list</i></b>	Enter the keyword <code>ciphers</code> and then a space-delimited list of ciphers that the SSH server supports. The following ciphers are available. <ul style="list-style-type: none"><li>• 3des-cbc</li><li>• aes128-cbc</li><li>• aes192-cbc</li><li>• aes256-cbc</li><li>• aes128-ctr</li><li>• aes192-ctr</li><li>• aes256-ctr</li></ul> The default cipher list is used.

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

**mac *hmac-  
algorithm***

Enter the keyword `mac` then a space-delimited list of hash message authentication code (HMAC) algorithms supported by the SSH server for keying hashing for the message authentication.

The following HMAC algorithms are available:

- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-sha2-256`

When FIPS is enabled, the default HMAC algorithm is `hmac-sha1-96`.

When FIPS is not enabled, the default HMAC algorithms are the following:

- `hmac-md5`
- `hmac-md5-96`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-sha2-256`

**kex  
*key-exchange-  
algorithm***

Enter the keyword `kex` and then a space-delimited list of key exchange algorithms supported by the SSH server.

The following key exchange algorithms are available:

- `diffie-hellman-group-exchange-sha1`
- `diffie-hellman-group1-sha1`
- `diffie-hellman-group14-sha1`


When FIPS is enabled, the default key-exchange-algorithm is `diffie-hellman-group14-sha1`.

When FIPS is not enabled, the default key-exchange-algorithms are the following:

- `diffie-hellman-group-exchange-sha1`
- `diffie-hellman-group1-sha1,`
- `diffie-hellman-group14-sha1`

**port *port-number*** (OPTIONAL) Enter the keyword `port` then the port number of the listening port of the SSH server. The range is from 1 to 65535. The default is **22**.

**[version {1 | 2}]** (OPTIONAL) Enter the keyword `version` then the SSH version 1 or 2 to specify only SSHv1 or SSHv2.

 **NOTE:** If you enable FIPS mode, you can only select version 2.

**Defaults** Default listening port is **22**.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the <code>cipher</code> , <code>kex</code> and <code>mac</code> options on the MXL 10/40GbE Switch.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 dns enable

Enable or disable the DNS in SSH server configuration to resolve hostname for host-based authentication.

**Syntax** `ip ssh server dns enable`  
To disable the DNS in SSH server configuration, use the `no ip ssh server dns enable` command.

 **NOTE:**  
This command is applicable only in Full-Switch mode.

**Defaults** Disabled.

**Command Modes** CONFIGURATION

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

<b>Version</b>	<b>Description</b>
<b>9.13.0.1</b>	Introduced on the MXL, C9010, S3048-ON, S3100 series, S4810, S4820T, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6100-ON, S6010-ON, Z9500, Z9100-ON and FN-IOM.

**Usage Information** To disable the DNS in SSH server configuration, use the `no ip ssh server dns enable` command.

## show crypto

Displays the public part of the SSH host-keys.

**Syntax** `show crypto key mypubkey {rsa | rsa1}`

<b>Parameters</b>	<b>Key</b>	
	<b>key</b>	Enter the keyword <code>key</code> to display the host public key.
	<b>mypubkey</b>	Enter the keyword <code>mypubkey</code> to display the host public key.
	<b>rsa</b>	Enter the keyword <code>rsa</code> to display the host SSHv2 RSA public key.
	<b>rsa1</b>	Enter the keyword <code>rsa1</code> to display the host SSHv1 RSA public key.

**Defaults** none  
**Command Modes** EXEC  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

#### Example

```
Dell#show crypto key mypubkey rsa1
1024 65537 150477578329696762034442
036788963493870885070479991994
81529207062670596651487238987338851
388872604558748599801007073218
241492903069202754403378383368480816
50517187573884981716247894646
7706560683627207710939806628138071534
8265219018664838324451688712
0415316302457397744496043353643022514
81307373438756957374121

Dell#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQ
C9IYgcUcc8wQm+5KUQgW/zAs8V5S
TalGq4/+S+6H9axpQnA+A0xweeo5iR5hvPP6Vc+
HS+uWoQH+VOJ8H5Jxsm347XnYv/
gpSghgjZ/C5UwFiucVkVfYu8RDcJViuQhLvPEeb
IF5Q+sD8K89MXU90MAS/UdoiJZSO
IlbaCuSTWlQ==
Dell#
```

**Related Commands** [crypto key generate](#) — generates the SSH keys.

## show ip ssh

Display information about established SSH sessions.

**Syntax** show ip ssh

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.10(0.0)</b>	Removed the support for hmac-sha2-256-96 algorithm.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

#### 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-sha2-256, hmac-sha1, hmac-sha1-96,
```

```

hmac-md5, hmac-md5-96.
SSH server kex algorithms : diffie-hellman-group-exchange-sha1,diffie-
hellman-group1-sha1,diffie-hellman-group14-sha1.
Password Authentication : enabled.
Hostbased Authentication : disabled.
RSA Authentication : disabled.
  Vty      Encryption      HMAC      Remote IP
  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** [show ip ssh client-pub-keys](#) — displays the client-public keys.

## show ip ssh client-pub-keys

Displays the client public keys used in host-based authentication

**Syntax** `show ip ssh client-pub-keys`

**Defaults** none

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

**Example**

```

Dell#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoiETH09G4sNV+ui+DWEc3cgYAcU5LailMU20DrzhCwyDNp05tKBU3tRe
o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdhf3Lk4D460HZRhhVrxqeNxPDpEnWIMPJ
ds= ashwani@poclab4

Dell#

```

## show ip ssh rsa-authentication

Displays 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

### 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
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHivMc1VZd0Sg5
GQxRV1y1X1JOMeO6Nd0WuYzrQMM4qJAoBwtneOXfLBcHF3V2hcMIqa
ZN+CRcnw/zCmlnCf0+qVTdloofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov
33m9+U9tMwhS8vy8AVxdH4x4km3c3t5Jvc=freedom@poclabb4
Dell#
```

## show role

Display information on permissions assigned to a command, including user role and/or permission level.

**Syntax** `show role mode {mode} {command}`

### Parameters

- command** Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.
- mode mode** Enter keyword then one of the following modes.
- configure
  - exec
  - interface
  - line
  - route-map
  - router

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
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](#) — creates user roles for the role-based security model.

## 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

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

**Related Commands** [userrole](#) — creates user roles for the role-based security model.

## ssh

Open an SSH connection specifying the host name, username, port number and version of the SSH client.

Dell Networking OS supports both inbound and outbound SSH sessions using IPv4 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

**Syntax** `ssh {hostname | ipv4 address} [-l username | -p port-number|-v {1|2}]`

**Parameters**

<b>hostname</b>	(OPTIONAL) Enter the IP address or the host name of the remote device.
<b>ipv4 address</b>	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
<b>-l username</b>	(OPTIONAL) Enter the keyword <code>-l</code> followed by the user name used in this SSH session. The default is the user name of the user associated with the terminal.
<b>-p port-number</b>	(OPTIONAL) Enter the keyword <code>-p</code> followed by the port number. The range is from 1 to 65536. The default is <b>22</b> .
<b>-v {1   2}</b>	(OPTIONAL) Enter the keyword <code>-v</code> 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

**Supported Modes** All Modes

**Command History**

Version	Description
9.10(0.0)	Removed the support for hmac-sha2-256-96 algorithm.
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

## Example

```
Dell#ssh 123.12.1.123 -l ashwani -p 5005 -v 2
```

## ip ssh pub-key-file

Specify the file used for host-based authentication.

**Syntax** `ip ssh pub-key-file {WORD}`

**Parameters** **WORD** Enter the file name for the host-based authentication.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

### Command History


Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Usage Information

This command specifies the file used for the host-based authentication. The `creates/` file overwrites the `flash://ADMIN_DIR/ssh/knownhosts` file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.

The file contains the OpenSSH-compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tK
BU3t
ReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdhf3Lk4D460HZRhhVrxqeNx
PDpEn 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.

## Secure DHCP Commands

The dynamic host configuration protocol (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** `clear ip dhcp snooping binding`

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch



<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**     [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.

## ip dhcp relay

Enable Option 82.

<b>Syntax</b>	<code>ip dhcp relay information-option [trust-downstream]</code>	
<b>Parameters</b>	<b>trust-downstream</b>	Configure the system to trust Option 82 when it is received from the previous-hop router.
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip dhcp snooping

Enable DHCP Snooping globally.

<b>Syntax</b>	<code>[no] ip dhcp snooping</code>
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 database

Delay writing the binding table for a specified time.

<b>Syntax</b>	<code>ip dhcp snooping database write-delay <i>minutes</i></code>	
<b>Parameters</b>	<b><i>minutes</i></b>	The range is from 5 to 21600.

**Defaults** none  
**Command Modes** CONFIGURATION  
**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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		
<b>mac <i>address</i></b>		Enter the keyword <code>mac</code> then the MAC address of the host to which the server is leasing the IP address.
<b>vlan-id <i>vlan-id</i></b>		Enter the keywords <code>vlan-id</code> then the VLAN to which the host belongs. The range is from 2 to 4094.
<b>ip <i>ip-address</i></b>		Enter the keyword <code>ip</code> then the IP address that the server is leasing.
<b>interface <i>type</i></b>		Enter the keyword <code>interface</code> then the type of interface to which the host is connected. <ul style="list-style-type: none"><li>For a ten-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>.</li></ul>
<b><i>slot/port</i></b>		Enter the slot and port number of the interface.
<b>lease <i>time</i></b>		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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.19.0</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip dhcp snooping trust

Configure an interface as trusted.

<b>Syntax</b>	[no] ip dhcp snooping trust
<b>Defaults</b>	Untrusted
<b>Command Modes</b>	INTERFACE
<b>Supported Modes</b>	Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ip dhcp source-address-validation

Enable IP source guard.

<b>Syntax</b>	[no] ip dhcp source-address-validation
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	INTERFACE
<b>Supported Modes</b>	Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.


## ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

<b>Syntax</b>	[no] ip dhcp snooping vlan <i>name</i>
<b>Parameters</b>	<i>name</i> Enter the name of a VLAN on which to enable DHCP Snooping.
<b>Defaults</b>	Disabled.
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Related Commands

[clear ip dhcp snooping](#) — clears the contents of the DHCP binding table.

## username

Establish an authentication system based on user names.

**Syntax** `username name [nopassword | {password | secret} [encryption-type] password] [privilege level]`

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

<b><i>name</i></b>	Enter a text string for the name of the user up to 63 characters.
<b><i>nopassword</i></b>	Enter the keyword <code>nopassword</code> to specify that the user should not enter a password.
<b><i>password</i></b>	Enter the keyword <code>password</code> followed by the <code>encryption-type</code> or the password.
<b><i>secret</i></b>	Enter the keyword <code>secret</code> followed by the <code>encryption-type</code> or the password.
<b><i>encryption-type</i></b>	Enter an encryption type for the <code>password</code> that you enter. <ul style="list-style-type: none"><li>• 0 directs Dell Networking OS to store the password as clear text. It is the default encryption type when using the <code>password</code> option.</li><li>• 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.</li><li>• 5 to indicate that a password encrypted using an MD5 hashing algorithm follow. This encryption type is available with the <code>secret</code> option only, and is the default encryption type for this option.</li></ul>
<b><i>password</i></b>	Enter a string up to 32 characters long.
<b><i>privilege level</i></b>	Enter the keyword <code>privilege</code> then a number from zero (0) to 15.
<b><i>secret</i></b>	Enter the keyword <code>secret</code> then the encryption type.

**Defaults** The default encryption type for the `password` option is **0**. The default encryption type for the `secret` option is **0**.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

**Usage Information**

To view the defined user names, use the `show running-config user` command.

**Related Commands**

[service password-encryption](#) — specifies a password for users on terminal lines.

[show running-config](#) — views the current configuration.

## 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**

***name***

Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).

***inherit existing-role-name***

Enter the `inherit` keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

**Defaults**

none

**Command Modes**

CONFIGURATION

**Supported Modes**

Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**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.

## ICMP Vulnerabilities

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. Dell Networking OS mainly addresses the following ICMP vulnerabilities:

- ICMP Mask Reply
- ICMP Timestamp Request
- ICMP Replies
- IP ID Values Randomness

You can configure the Dell Networking OS to drop ICMP reply messages. When you configure the `drop icmp` command, the system drops the ICMP reply messages from the front end and management interfaces. By default, the Dell Networking OS responds to all the ICMP messages. The Dell Networking OS suppresses the following ICMPv4 and ICMPv6 message types:

**Table 4. Suppressed ICMPv4 message types**

ICMPv4 Message Types
Echo reply (0)
All sub types of destination unreachable (3)
Source quench (4)
Redirect (5)
Router advertisement (9)
Router solicitation (10)
Time exceeded (11)
IP header bad (12)
Timestamp request (13)
Timestamp reply (14)
Information request (15)
Information reply (16)
Address mask request (17)
Address mask reply (18)

**NOTE:** The Dell Networking OS does not suppress the **ICMPv4** message type `Echo request (8)`.

**Table 5. Suppressed ICMPv6 message types**

ICMPv6 Message Types
Destination unreachable (1)
Time exceeded (3)
IPv6 header bad (4)
Echo reply (129)
Who are you request (139)

**Table 5. Suppressed ICMPv6 message types (continued)**

ICMPv6 Message Types
Who are you reply (140)
Mtrace response (200)
Mtrace messages (201)

**NOTE:**

The Dell Networking OS does not suppress the following **ICMPv6** message types:

- Packet too big (2)
- Echo request (128)
- Multicast listener query (130)
- Multicast listener report (131)
- Multicast listener done (132)
- Router solicitation (133)
- Router advertisement (134)
- Neighbor solicitation (135)
- Neighbor advertisement (136)
- Redirect (137)
- Router renumbering (138)
- MLD v2 listener report (143)
- Duplicate Address Request (157)
- Duplicate Address Confirmation (158)

## drop icmp

Drops the ICMPv4 and ICMPv6 packets.

**Syntax** `drop {icmp | icmp6}`

**Command Modes** CONFIGURATION

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

Version	Description
---------	-------------

<b>9.11.0.0</b>	Introduced on the S4810, S4820T, S3048-ON, S3100 Series, S4048-ON, S5000, S6000, S6000-ON, Z9500, Z9100-ON, S6100-ON, S6010-ON, S4048T-ON, C9000, M IOA, FN IOM, and MXL.
-----------------	---

**Usage Information** When the `drop icmp` feature is configured, the system drops the ICMP reply messages on the front end and management interfaces. By default, the Dell Networking OS responds to all the ICMP messages.

**NOTE:** There is no separate CLI to enable IP ID randomness. By default, the IP ID in the kernel is randomized.

## System Security Commands

The following section lists the system security commands.

## generate hash

Generate a hash checksum for the given file or the startup configuration using the MD5, SHA1, or SHA256 algorithm.

<b>Syntax</b>	<code>generate hash {md5   sha1   sha256} {flash://filename   startup-config}</code>	
<b>Parameters</b>	<b>md5   sha1   sha256</b>	Enter the keyword <code>md5</code> , <code>sha1</code> , or <code>sha256</code> to generate .
	<b>flash:// filename</b>	Enter the keyword <code>flash:</code> and enter the filename to generate the hash checksum for any file in the flash drive using the MD5, SHA1, or SHA256 algorithm.
	<b>startup-config</b>	Enter the keyword <code>shartup-config</code> to generate the hash checksum for the startup configuration using the MD5, SHA1, or SHA256 algorithm.
<b>Defaults</b>	None	
<b>Command Modes</b>	EXEC Privilege	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
	<b>9.14(0.0)</b>	Introduced on the S5048F-ON.
	<b>9.13(0.0)</b>	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, Z9500, C9010, MXL, and FN-IOM.
<b>Usage Information</b>	Use the <code>generate hash</code> command to generate a hash checksum for your startup configuration, and use the hash to verify using the <code>verified boot hash</code> command.	

### Example

```
DellEMC#generate hash md5 startup-config
MD5SUM(/f10/flash/startup-config) : f81812a64eea202c5b2ef782639bafc3
```

## root-access password

Configure the root access password.

<b>Syntax</b>	<code>root-access password [encryption-type] root-password</code> To reset to the default password, use the <code>no root-access password</code> command.	
<b>Parameters</b>	<b>encryption-type</b>	(OPTIONAL) Enter an encryption type for the root password that you enter. <ul style="list-style-type: none"><li>• 0 directs the system to store the password as clear text.</li><li>• 7 directs the system to store the password with a dynamic salt.</li><li>• 9 directs the system to encrypt the clear text password and store the encrypted password in an inaccessible location.</li></ul>
	<b>root-password</b>	Enter the root password.
<b>Defaults</b>	Not configured	
<b>Command Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.14(1.0)</b>	Introduced on the S4810 and S4820T.
	<b>9.14(0.0)</b>	Introduced on the S5048F-ON.



Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, Z9500, C9010, MXL, and FN-IOM.

### Usage Information

If you configure the `secure-cli` command on the system, the Dell EMC Networking OS resets any previously-configured root access password to the default root password without displaying any warning message. With the `secure-cli` command enabled on the system, the CONFIGURATION mode does not display the `root access password` option.

When you configure the root access password, ensure that your password meets the following criteria:

- A minimum of eight characters in length
- A minimum of one lower case letter (a to z)
- A minimum of one upper case letter (A to Z)
- A minimum of one numeric character (0 to 9)
- A minimum of one special character including a space (" !"#\$\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~")

If your password does not meet the criteria, the system does not accept your password.

If you use encryption type 9, the system stores the clear text password in an inaccessible location on the system. The `show running-configuration` command does not display the password. This configuration is not portable between different systems.

### Example

```
DellEMC)# show running-config | g root
root-access password 7
f4dc0cb9787722dd1084d17f417f164cc7f730d4f03d4f0215294cbd899614e3
```

## verified boot

Enable OS image hash validation during system startup.

### Syntax

```
verified boot
```

To disable OS image hash validation, use the `no verified boot` command.

### Defaults

Not configured

### Command Modes

CONFIGURATION

### Command History

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.14(0.0)	Introduced on the S5048F-ON.
9.13(0.0)	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, MXL, and FN-IOM.

### Usage Information

When you reboot the system using the `reload` command, the system performs OS image verification on the primary boot image. You can enable boot image hash validation only for images on local flash partitions such as A: or B:.

### Example

```
DellEMC(config)# verified boot
```

## verified boot hash

Verify and store the hash value of the startup configuration.

### Syntax

```
verified boot hash {system-image {A: | B:} | startup-config} hash value
```

## Parameters

**system-image {A: | B:}** Enter the keyword `system-image` and A: or B:, depending on where the image is stored and then the hash value that is present on the iSupport page for your image.

**startup-config** Enter the keyword `startup-config` and then the hash value for the startup configuration. You can get the hash value for the startup configuration using the `generate hash` command.

**hash value** Enter the MD5, SHA1, or SHA256 hash.

**Defaults** None

**Command Modes** EXEC Privilege

## Command History

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.14(0.0)	Introduced on the S5048F-ON.
9.13(0.0)	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, Z9500, C9010, MXL, and FN-IOM.

## Usage Information

Dell EMC Networking OS supports MD5, SHA1, and SHA256.

## Example

```
DellEMC# verified boot hash system-image A:  
619A8C1B7A2BC9692A221E2151B9DA9E
```

## verified startup-config

Enable hash validation for the startup configuration during system startup.

## Syntax

```
verified startup-config
```

To disable hash validation for the startup configuration, use the `no verified startup-config` command.

**Defaults** Not configured

**Command Modes** Full-Switch

## Command History

Version	Description
9.14(1.0)	Introduced on the S4810 and S4820T.
9.14(0.0)	Introduced on the S5048F-ON.
9.13(0.0)	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5000, S6000, S6000-ON, S6010-ON, S6100-ON, Z9100-ON, Z9500, C9010, MXL, and FN-IOM.

## Example

```
DellEMC(config)# verified startup-config
```

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 OS 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.
- The system 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.
- 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 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](#)).
  - 1600 packets when you enable extended-router and/or extended-gateway information packing

### Topics:

- [sflow collector](#)
- [sflow enable \(Global\)](#)
- [sflow ingress-enable](#)
- [sflow extended-switch enable](#)
- [sflow max-header-size extended](#)
- [sflow polling-interval \(Global\)](#)
- [sflow polling-interval \(Interface\)](#)
- [sflow sample-rate \(Global\)](#)
- [sflow sample-rate \(Interface\)](#)
- [show sflow](#)
- [show sflow stack-unit](#)

## sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

**Syntax** `sflow collector {ip-address} agent-addr {ip-address} [number [max-datagram-size number]] | [max-datagram-size number]`

To delete a configured collector, use the `no sflow collector {ip-address} agent-addr {ipv4-address} [number [max-datagram-size number]] | [max-datagram-size number]` command.

<b>Parameters</b>	<b>sflow collector</b> <i>ip-address</i>	Enter the IPv4 (A.B.C.D) of the sFlow collector device.
	<b>agent-addr</b> <i>ip-address</i>	Enter the IPv4 (A.B.C.D) of the sFlow agent in the router.
	<b>number</b>	(OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is from 0 to 65535. The default is 6343.
	<b>max-datagram-size</b> <i>number</i>	(OPTIONAL) Enter the keyword max-datagram-size then the size number in bytes. The range is from 400 to 1500. The default is <b>1400</b> .
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch Mode	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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, the system returns the corresponding configured agent IP in the MIB requests. The system checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, the system generates the following error: <code>%Error: Different agent-addr attempted for an existing collector.</code>	

## sflow enable (Global)

Enable sFlow globally.

<b>Syntax</b>	<code>sflow enable</code>	
	To disable sFlow, use the <code>no sflow enable</code> command.	
<b>Defaults</b>	Disabled.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch Mode	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	sFlow is disabled by default. In addition to this command, you must enable sFlow on individual interfaces where you want sFlow sampling.	

**Related Commands** [sflow enable \(Global\)](#) — 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

**Supported Modes** Full-Switch 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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the 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

**Supported Modes** Full-Switch Mode

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The Dell Networking OS version 7.8.1.0 and later enhances the sflow implementation for real time traffic analysis 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
- Supported Modes** Full-Switch Mode
- Command History** This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.  
The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on the MXL switch.

### 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
- Supported Modes** Full-Switch Mode
- Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
- 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.

## sflow polling-interval (Interface)

Set the sFlow polling interval at an interface (overrides the global-level setting).

<b>Syntax</b>	<code>sflow polling-interval interval value</code> To return to the default, use the <code>no sflow polling-interval interval</code> command.						
<b>Parameters</b>	<b>interval value</b> Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is <b>the global counter polling interval</b> .						
<b>Defaults</b>	The same value as the current global default counter polling interval.						
<b>Command Modes</b>	INTERFACE						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	This command sets the counter polling interval for an interface.						
<b>Related Commands</b>	<a href="#">sflow polling-interval (Global)</a> — globally sets the polling interval.						

## sflow sample-rate (Global)

Change the global default sampling rate.

<b>Syntax</b>	<code>sflow sample-rate value</code> To return to the default sampling rate, use the <code>no sflow sample-rate</code> command.						
<b>Parameters</b>	<b>value</b> Enter the sampling rate value. 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 <b>32768 packets</b> .						
<b>Defaults</b>	<b>32768 packets</b>						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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.						
<b>Related Commands</b>	<a href="#">sflow sample-rate (Interface)</a> — changes the interface sampling rate.						

# sflow sample-rate (Interface)

Change the interface default sampling rate.

<b>Syntax</b>	<code>sflow sample-rate value</code> To return to the default sampling rate, use the <code>no sflow sample-rate</code> command.						
<b>Parameters</b>	<b>value</b> Enter the sampling rate value. The range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, and 16384. The default is <b>the Global default sampling</b> .						
<b>Defaults</b>	The Global default sampling.						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	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 you enter is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two numbers and re-enter the command.						
<b>Related Commands</b>	<a href="#">sflow sample-rate (Global)</a> — changes the sampling rate globally.						

## show sflow

Display the current sFlow configuration.

<b>Syntax</b>	<code>show sflow [interface]</code>						
<b>Parameters</b>	<b>interface</b> (OPTIONAL) Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"><li>For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li><li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul>						
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	The <code>dropEvent</code> counter (sFlow samples dropped due to sub-sampling) shown in the following example always displays a value of zero.						
<b>Example</b>	<pre>Dell#show sflow sFlow services are enabled Egress Mangement Interface sFlow services are disabled Global default sampling rate: 2048 Global default counter polling interval: 20 Global extended information enabled: none</pre>						



```

0 collectors configured
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected

stack-unit 0 Port set 0
  Te 0/1: configured rate 256, actual rate 256
Dell#
Dell#show running-config sflow
!
sflow enable
sflow sample-rate 2048
Dell#show running-config interface tengigabitethernet 0/1
!
interface TenGigabitEthernet 0/1
  no ip address
  sflow enable
  sflow sample-rate 256
  no shutdown

```

## show sflow stack-unit

Display the sFlow information on a stack unit.

**Syntax** `show sflow stack-unit {unit number}`

**Parameters** *unit number* (OPTIONAL) Enter a unit number to view information on the stack unit in that slot. The range is from 0 to 5.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example below always displays a value of zero.

### Example

```

Dell#show sflow stack-unit 1
Stack-Unit 1
  Samples rcvd from h/w      :0
  Total UDP packets exported :0
  UDP packets dropped       :0
Dell#

```

## 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*.

This chapter includes commands for the Dell Networking operating software Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

For more information, see [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, see [VLAN Stacking](#).
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol [LACP]) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.

#### Topics:

- [debug protocol-tunnel](#)
- [protocol-tunnel](#)
- [protocol-tunnel destination-mac](#)
- [protocol-tunnel enable](#)
- [protocol-tunnel rate-limit](#)
- [show protocol-tunnel](#)

### debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

**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

<b>interface</b>	Enter one of the following interfaces and slot/port information: <ul style="list-style-type: none"> <li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul>
<b>in   out   both</b>	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.
<b>vlan <i>vlan-id</i></b>	Enter the keyword <code>vlan</code> then the VLAN ID. The range is from 1 to 4094.
<b>count <i>value</i></b>	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  
**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**

<b>rate-limit <i>rate</i></b>	Enter the keyword <code>rate-limit</code> then a number for the rate-limit for tunneled packets on the VLAN. The range is from 64 to 320.
<b>stp</b>	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  
**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#conf
Dell(conf)#interface vlan 2
Dell(conf-if-vl-2)#vlan-stack compatible
Dell(conf-if-vl-2)#member Tel/2-3
Dell(conf-if-vl-2)#protocol-tunnel stp
Dell(conf-if-vl-2)#protocol-tunnel enable
```

**Related Command** [show protocol-tunnel](#) — displays tunneling information for all VLANs.

## protocol-tunnel destination-mac

Overwrite the BPDU destination MAC address with a specific value.

**Syntax** `protocol-tunnel destination-mac xstp address`

**Parameters**

<b>stp</b>	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  
**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system must have the default CAM profile with the default microcode before you enable L2PT.

## protocol-tunnel rate-limit

Enable traffic rate limiting per box.

**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** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
Dell#
Dell#conf
Dell(conf)#protocol-tunnel rate-limit 1000
Dell(conf)#
```

**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 *vlan-id*** (OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### 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
```

### Example (Specific VLAN)

```
Dell#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface  Vlan  Protocol(s)
Te1/2      2     STP, PVST
Dell#
```

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

# Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog.

The chapter contains the following sections:

- [SNMP Commands](#)
- [Syslog Commands](#)

## Topics:


- [SNMP Commands](#)
- [clear logging auditlog](#)
- [show snmp](#)
- [show snmp engineID](#)
- [show snmp group](#)
- [show snmp supported-mibs](#)
- [show snmp supported-traps](#)
- [show snmp user](#)
- [snmp context](#)
- [snmp context](#)
- [snmp ifmib ifalias long](#)
- [snmp-server community](#)
- [snmp-server contact](#)
- [snmp-server enable traps](#)
- [snmp-server engineID](#)
- [snmp-server group](#)
- [snmp-server host](#)
- [snmp-server location](#)
- [snmp-server packetsize](#)
- [snmp-server trap-source](#)
- [snmp-server user](#)
- [snmp-server user \(for AES128-CFB Encryption\)](#)
- [snmp-server view](#)
- [snmp trap link-status](#)
- [Syslog Commands](#)
- [clear logging](#)
- [default logging buffered](#)
- [default logging console](#)
- [logging extended](#)
- [default logging monitor](#)
- [default logging trap](#)
- [logging](#)
- [logging buffered](#)
- [logging console](#)
- [logging facility](#)
- [logging history](#)
- [logging history size](#)
- [logging monitor](#)
- [logging on](#)
- [logging source-interface](#)

- [logging synchronous](#)
- [logging trap](#)
- [logging version](#)
- [show logging](#)
- [show logging driverlog stack-unit](#)
- [show logging auditlog](#)
- [terminal monitor](#)

## 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. The system supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. The system sends SNMP traps, which are messages informing an SNMP management system about the network. The system supports up to 16 SNMP trap receivers.

 **NOTE:** The system does not support SNMPv3 traps in PMUX mode.

## Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both local area network (LAN) and wide area network (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 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).

## clear logging auditlog

Clears audit log.

**Syntax** `clear logging auditlog`

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch 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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.5(0.0)</b>	Introduced on the MXL.

### Example

```
Dell(conf)#clear logging auditlog
```

**Related Commands** [show logging auditlog](#) — displays audit log

# show snmp

Display the status of SNMP network elements.

**Syntax** show snmp

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

The following Example displays a group named *ngroup*. The *ngroup* has a security model of version 3 (v3) with authentication (*auth*), the read and notify name is *nview* with no write view name specified, and finally the row status is active.

**Example**

```
Dell#show snmp group
groupname: ngroup          security model: v3 auth
readview : nview          writeview: no write view specified
notifyview: nview
row status: active
Dell#
```

**Related Commands** [snmp-server group](#) — configures an SNMP server group.

## show snmp supported-mibs

Display the list of SNMP MIBs supported by the platform.

**Syntax** `show snmp supported-mibs`

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

Version	Description
<b>9.14(0.0)</b>	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048-ON, S3100, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON and Z9100-ON.

**Example**

```
DellEMC#show snmp supported-mibs
MIB                                OID
-----
RFC1155-SMI                        -
RFC-1212                            -
SNMPv2-SMI                          -
SNMPv2-TC                          -
SNMPv2-CONF                        -
INET-ADDRESS-MIB                   -
IANAifType-MIB                     -
```

```

IANA-ADDRESS-FAMILY-NUMBERS-MIB -
IANA-RTPROTO-MIB -
IPV6-FLOW-LABEL-MIB -
SNMPv2-MIB 1.3.6.1.2.1
IF-MIB 1.3.6.1.2.1.31
IP-MIB 1.3.6.1.2.1.48
TCP-MIB 1.3.6.1.2.1.49
UDP-MIB 1.3.6.1.2.1.50
RFC1213-MIB -
EtherLike-MIB 1.3.6.1.2.1.35
SNMP-FRAMEWORK-MIB 1.3.6.1.6.3.10
RADIUS-AUTH-CLIENT-MIB 1.3.6.1.2.1.67.1.2
SNMP-MPD-MIB 1.3.6.1.6.3.11
RMON-MIB 1.3.6.1.2.1.16
--More-

```

## show snmp supported-traps

Display the list of SNMP traps supported by the platform.

**Syntax** `show snmp supported-traps`

- Command Modes**
- EXEC
  - EXEC Privilege

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

Version	Description
<b>9.14(0.0)</b>	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048-ON, S3100, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON and Z9100-ON.

### Example

```

DellEMC#show snmp supported-traps
TRAP                                OID
-----
COLDSTART                           1.3.6.1.6.3.1.1.5.1
WARMSTART                           1.3.6.1.6.3.1.1.5.2
LINKDOWN                             1.3.6.1.6.3.1.1.5.3
LINKUP                               1.3.6.1.6.3.1.1.5.4
Authenticationfailure               1.3.6.1.6.3.1.1.5.5
dellNetIfAlarmHighBer               1.3.6.1.4.1.6027.3.11.1.4.1.1
dellNetIfAlarmHighBerClr            1.3.6.1.4.1.6027.3.11.1.4.1.2
dellNetSysAlarmCardDown             1.3.6.1.4.1.6027.3.26.1.5.1.1
dellNetSysAlarmCardUp               1.3.6.1.4.1.6027.3.26.1.5.1.2
dellNetSysAlarmCardOffline          1.3.6.1.4.1.6027.3.26.1.5.1.3
dellNetSysAlarmCardMismatch         1.3.6.1.4.1.6027.3.26.1.5.1.4
dellNetSysAlarmRpmUp                1.3.6.1.4.1.6027.3.26.1.5.1.5
dellNetSysAlarmRpmDown              1.3.6.1.4.1.6027.3.26.1.5.1.6
dellNetSysAlarmPowersupplyDown      1.3.6.1.4.1.6027.3.26.1.5.1.7
dellNetSysAlarmMinorTemperatureHigh 1.3.6.1.4.1.6027.3.26.1.5.1.8
dellNetSysAlarmMajorTemperatureHigh 1.3.6.1.4.1.6027.3.26.1.5.1.9
dellNetSysAlarmFanTrayDown          1.3.6.1.4.1.6027.3.26.1.5.1.10
dellNetSysAlarmPowersupplyClear     1.3.6.1.4.1.6027.3.26.1.5.1.11
dellNetSysAlarmMinorTemperatureClear 1.3.6.1.4.1.6027.3.26.1.5.1.12
dellNetSysAlarmMajorTemperatureClear 1.3.6.1.4.1.6027.3.26.1.5.1.13
dellNetSysAlarmFanTrayClear         1.3.6.1.4.1.6027.3.26.1.5.1.14
--More-

```

# show snmp user

Display the information configured on each SNMP user name.

**Syntax** `show snmp user`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show snmp user
  User name: v1v2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile      active
  Authentication Protocol: None
  Privacy Protocol: None

Dell#
```

# snmp context

Enables you to map a BGP VRF instance within an SNMP context through community mapping in SNMPv2c and SNMPv3.

**Syntax** `[no] snmp context [context name]`

**Parameters**

<b>context name</b>	Enter a unique name for the context.
---------------------	--------------------------------------

**Defaults** None

**Command Modes** CONFIGURATION

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

Version	Description
<b>9.14.1.0</b>	Introduced on S4810 and S4820T.
<b>9.13(0.0)</b>	Introduced on all DNOS platforms.

**Usage Information** Use this command to map SNMP context to a VRF instance within a community in SNMPv2c and SNMPv3. The no version of this command turns off this feature.

# snmp context

Configure SNMPv3 context name to map multiple OSPFv3 VRF instances.

**Syntax** `snmp context {context-name}`  
To clear snmp context, use the `no snmp context {context-name}` command.

**Parameters**

<b>context-name</b>	Enter the SNMP context name. The maximum length is 32 alphanumeric characters.
---------------------	--

<b>Defaults</b>	None.
<b>Command Modes</b>	IPv6 ROUTER OSPF
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .
<b>Version</b>	<b>Description</b>
<b>9.14(1.0)</b>	Introduced on the S3100 series, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6010-ON, S6100-ON, Z9100-ON, Z9500, S6000-ON, C9010, MXL, and FN IOM.

**Usage Information** Use SNMPv3 context configuration to distinguish between various OSPFv3 VRF instances.

**Example**

```
DellEMC(conf-ipv6-router_ospf)#snmp context ospf1
```

```
DellEMC>show runnig-config ospf
!
ipv6 router ospf 10
  router-id 10.10.10.1
  snmp context ospf1
!
DellEMC>
```

## snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

<b>Syntax</b>	snmp ifmib ifalias long
<b>Defaults</b>	Interface description truncated beyond 63 characters.
<b>Command Modes</b>	CONFIGURATION
<b>Supported Modes</b>	Full-Switch Mode

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
!----command run on host connected to switch:-----!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2.
This is a
port connected to
IF-MIB::ifAlias.134792448 = STRING:

!----command run on Force10 switch:-----!
Dell#snmp ifmib ifalias long

!----command run on server connected to switch:-----!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2.
This is a
port connected to Router2. This is a port connected to Router2. This is
a port
connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
```

# snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

**Syntax** `snmp-server community community-name {ro | rw} [security-name name][access-list-name]`

To remove access to a community, use the `no snmp-server community community-string {ro | rw} [security-name name [access-list-name]` command.

**Parameters**

- community-name*** Enter a text string (up to 20 characters long) to act as a password for SNMP.
- ro** Enter the keyword `ro` to specify read-only permission.
- rw** Enter the keyword `rw` to specify read-write permission.
- security-name name*** (Optional) Enter the keywords `security-name` then the security name as defined by the community MIB.
- access-list-name*** (Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

[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** *text* Enter an alphanumeric text string, up to 55 characters long.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

<b><i>notification-type</i></b>	Enter the type of notification from the following list: <ul style="list-style-type: none"><li>• <code>ecfm</code> — Notification of changes to ECFM.</li><li>• <code>entity</code> — Notification of changes to entity.</li><li>• <code>envmon</code> — For Dell Networking device notifications when an environmental threshold is exceeded.</li><li>• <code>eoam</code> — Notification of changes to the EOAM state.</li><li>• <code>ets</code> — Notification of changes to the ets traps.</li><li>• <code>fips</code> — Notification of changes to the FIP snooping state.</li><li>• <code>lACP</code> — Notification of changes.</li><li>• <code>pfc</code> — Notification of changes to pfc traps.</li><li>• <code>snmp</code> — Notification of RFC 1157 traps.</li><li>• <code>stp</code> — Notification of a state change in the spanning tree protocol (RFC 1493).</li><li>• <code>vrrp</code> — Notification of a state change in a VRRP group.</li><li>• <code>xstp</code> — Notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.</li></ul>
---------------------------------	---

***notification-option*** For the `envmon` notification-type, enter one of the following optional parameters:

- `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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Added the following two SNMP notification options: <code>syslog-reachable</code> and <code>syslog-unreachable</code> .
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The system supports up to 16 SNMP trap receivers.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

**Related Commands** [snmp-server community](#) — enables SNMP and sets the community string.

## snmp-server 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 `local` then the engine ID number that identifies the copy of the SNMP on the local device.

Format (as specified in RFC 3411): 12 octets.

- The first four octets are set to the private enterprise number.
- The remaining eight octets are the MAC address of the chassis.

**remote ip-address** Enter the keyword `remote` then the IP address that identifies the copy of the SNMP on the remote device.

**udp-port port-number engineID** Enter the keywords `udp-port` then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is **162**.

**Defaults** As above.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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 you must reconfigure the users.

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` — 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-list-name | 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-list-name | access-list-name]` command.

## Parameters


<b>group_name</b>	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): <ul style="list-style-type: none"><li>• <code>v1v2creadg</code> — maps to a community/security-name with <code>ro</code> permissions.</li><li>• <code>1v2cwriteg</code> — maps to a community/security-name <code>rw</code> permissions.</li></ul>
<b>1   2c   3</b>	(OPTIONAL) Enter the security model version number (1, 2c, or 3): <ul style="list-style-type: none"><li>• 1 is the least secure version.</li><li>• 3 is the most secure of the security modes.</li><li>• 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.</li></ul> The default is <b>1</b> .
<b>auth</b>	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.
<b>noauth</b>	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.
<b>priv</b>	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.
<b>read name</b>	(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 <b>GlobalView</b> and is assumed to be every object belonging to the internet (1.3.6.1) OID space.
<b>write name</b>	(OPTIONAL) Enter the keyword <code>write</code> then a name (a string of up to 20 characters long) as the write view name.
<b>notify name</b>	(OPTIONAL) Enter the keyword <code>notify</code> then a name (a string of up to 20 characters long) as the notify view name.
<b>access-list-name</b>	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

**Defaults** As above.

**Command Modes** CONFIGURATION




**Supported Modes** Full-Switch Mode



<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;">Version</th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td>9.9(0.0)</td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td>8.3.16.1</td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	Version	Description	9.9(0.0)	Introduced on the FN IOM.	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
9.9(0.0)	Introduced on the FN IOM.						
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>The following Example specifies the group named <i>harig</i> as a version 3 user requiring both authentication and encryption and read access limited to the read named <i>rview</i>.</p> <p> <b>NOTE:</b> The number of configurable groups is limited to 16 groups.</p>						
<b>Example</b>	<pre>Dell#conf Dell(conf)# snmp-server group harig 3 priv read rview Dell#</pre>						
<b>Related Commands</b>	<p><a href="#">show snmp group</a> — displays the group name, security model, view status, and storage type of each group.</p> <p><a href="#">show running-config</a> — displays the SNMP running configuration.</p>						

## snmp-server host

Configure the recipient of an SNMP trap operation.

<b>Syntax</b>	<pre>snmp-server host ip-address [traps   informs] [version 1   2c   3] [auth   no auth   priv] [community-string] [udp-port port-number] [notification-type]</pre> <p>To remove the SNMP host, use the <code>no snmp-server host ip-address [traps   informs] [version 1   2c   3] [auth   noauth   priv] [community-string] [udp-port number] [notification-type]</code> command.</p>																
<b>Parameters</b>	<table border="0"> <tr> <td style="vertical-align: top;"><b><i>ip-address</i></b></td> <td>Enter the keyword <code>host</code> then the IP address of the host (configurable hosts is limited to 16).</td> </tr> <tr> <td style="vertical-align: top;"><b><i>traps</i></b></td> <td>(OPTIONAL) Enter the keyword <code>traps</code> to send trap notifications to the specified host. The default is <b><code>traps</code></b>.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>informs</i></b></td> <td>(OPTIONAL) Enter the keyword <code>informs</code> to send inform notifications to the specified host. The default is <b><code>traps</code></b>.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>version 1   2c   3</i></b></td> <td>           (OPTIONAL) Enter the keyword <code>version</code> to specify the security model then the security model version number 1, 2c, or 3:           <ul style="list-style-type: none"> <li>• Version 1 is the least secure version.</li> <li>• Version 3 is the most secure of the security modes.</li> <li>• Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.</li> </ul>           The default is version <b>1</b>.         </td> </tr> <tr> <td style="vertical-align: top;"><b><i>auth</i></b></td> <td>(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>noauth</i></b></td> <td>(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>priv</i></b></td> <td>(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.</td> </tr> <tr> <td style="vertical-align: top;"><b><i>community-string</i></b></td> <td>           Enter a text string (up to 20 characters long) as the name of the SNMP community.           <p> <b>NOTE:</b> 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</p> </td> </tr> </table>	<b><i>ip-address</i></b>	Enter the keyword <code>host</code> then the IP address of the host (configurable hosts is limited to 16).	<b><i>traps</i></b>	(OPTIONAL) Enter the keyword <code>traps</code> to send trap notifications to the specified host. The default is <b><code>traps</code></b> .	<b><i>informs</i></b>	(OPTIONAL) Enter the keyword <code>informs</code> to send inform notifications to the specified host. The default is <b><code>traps</code></b> .	<b><i>version 1   2c   3</i></b>	(OPTIONAL) Enter the keyword <code>version</code> to specify the security model then the security model version number 1, 2c, or 3: <ul style="list-style-type: none"> <li>• Version 1 is the least secure version.</li> <li>• Version 3 is the most secure of the security modes.</li> <li>• Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.</li> </ul> The default is version <b>1</b> .	<b><i>auth</i></b>	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.	<b><i>noauth</i></b>	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.	<b><i>priv</i></b>	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.	<b><i>community-string</i></b>	Enter a text string (up to 20 characters long) as the name of the SNMP community. <p> <b>NOTE:</b> 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</p>
<b><i>ip-address</i></b>	Enter the keyword <code>host</code> then the IP address of the host (configurable hosts is limited to 16).																
<b><i>traps</i></b>	(OPTIONAL) Enter the keyword <code>traps</code> to send trap notifications to the specified host. The default is <b><code>traps</code></b> .																
<b><i>informs</i></b>	(OPTIONAL) Enter the keyword <code>informs</code> to send inform notifications to the specified host. The default is <b><code>traps</code></b> .																
<b><i>version 1   2c   3</i></b>	(OPTIONAL) Enter the keyword <code>version</code> to specify the security model then the security model version number 1, 2c, or 3: <ul style="list-style-type: none"> <li>• Version 1 is the least secure version.</li> <li>• Version 3 is the most secure of the security modes.</li> <li>• Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.</li> </ul> The default is version <b>1</b> .																
<b><i>auth</i></b>	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.																
<b><i>noauth</i></b>	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.																
<b><i>priv</i></b>	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.																
<b><i>community-string</i></b>	Enter a text string (up to 20 characters long) as the name of the SNMP community. <p> <b>NOTE:</b> 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</p>																

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` then 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 send to the host:

- `ecfm` — Notification of ECFM state changes.
- `entity` — Notification of entity changes.
- `envmon` — Environment monitor trap.
- `eoam` — Notification of EOAM state changes.
- `ets` — Notification of ets trap changes.
- `fips` — Notification of FIP snooping state changes.
- `lACP` — Notification of LACP state changes.
- `snmp` — SNMP notification (RFC 1157).
- `stp` — Spanning tree protocol notification (RFC 1493).
- `vrrp` — State change in a VRRP group.
- `xstp` — State change in MSTP (802.1s), RSTP (802.1w), and PVST+.

The default is all trap types are sent to host.

**Defaults** As above.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 is 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.

<b>Syntax</b>	<code>snmp-server location text</code>	
	To delete the SNMP location, use the <code>no snmp-server location</code> command.	
<b>Parameters</b>	<b>text</b>	Enter an alpha-numeric text string, up to 55 characters long.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch Mode	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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.

<b>Syntax</b>	<code>snmp-server packetsize byte-count</code>	
<b>Parameters</b>	<b>byte-count</b>	Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.
<b>Defaults</b>	<b>8</b>	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch Mode	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

<b>Syntax</b>	<code>snmp-server trap-source interface</code>	
	To disable sending traps out a specific interface, use the <code>no snmp trap-source</code> command.	
<b>Parameters</b>	<b>interface</b>	Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** The IP address assigned to the management interface is the default.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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-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]` command.

Parameters		
<b><i>name</i></b>		Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.
<b><i>group_name</i></b>		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): <ul style="list-style-type: none"> <li>• <code>v1v2creadu</code> — maps to a community with <code>ro</code> permissions.</li> <li>• <code>1v2cwriteu</code> — maps to a community <code>rw</code> permissions.</li> </ul>
<b><i>remote ip-address</i></b>		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 <b>162</b> .
<b><i>udp-port port-number</i></b>		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 <b>162</b> .
<b><i>1   2c   3</i></b>	(OPTIONAL)	Enter the security model version number (1, 2c, or 3): <ul style="list-style-type: none"> <li>• 1 is the least secure version.</li> <li>• 3 is the most secure of the security modes.</li> <li>• 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.</li> </ul> The default is <b>1</b> .
<b><i>encrypted</i></b>	(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).
<b><i>auth</i></b>	(OPTIONAL)	Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.

<b>md5   sha</b>	(OPTIONAL) Enter the keyword <code>md5</code> or <code>sha</code> to designate the authentication level. <ul style="list-style-type: none"> <li>• <code>md5</code> — Message Digest Algorithm</li> <li>• <code>sha</code> — Secure Hash Algorithm</li> </ul>
<b>auth-password</b>	(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.
<b>priv des56</b>	(OPTIONAL) Enter the keywords <code>priv des56</code> to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm ( <code>des56</code> ).
<b>aes128</b>	(OPTIONAL) Enter the keyword <code>aes128</code> to initiate the AES128-CFB encryption algorithm for transmission of SNMP packets.
<b>priv password</b>	(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 decrypt the contents of the message it receives from the agent. Minimum: eight characters long.
<b>access-list-name</b>	(Optional) Enter the standard IPv4 access list name (a string up to 16 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

**Supported Modes** Full-Switch Mode


**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.3(0.0)</b>	Added support for the AES128-CFB encryption algorithm on the MXL 10/40GbE Switch IO Module platform.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

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

- auth-password*** (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.
- aes128*** (OPTIONAL) Enter the keyword `aes128` to initiate the AES128-CFB encryption algorithm for transmission of SNMP packets.
- 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 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

**Supported Modes** Full-Switch Mode

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.3(0.0)	Added support for the AES128-CFB encryption algorithm on the MXL 10/40GbE Switch IO Module platform
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

<b><i>view-name</i></b>	Enter the name of the view (not to exceed 20 characters).
<b><i>oid-tree</i></b>	Enter the OID sub tree for the view (not to exceed 20 characters).
<b>included</b>	(OPTIONAL) Enter the keyword <code>included</code> to include the MIB family in the view.
<b>excluded</b>	(OPTIONAL) Enter the keyword <code>excluded</code> to exclude the MIB family in the view.

## Defaults

none

## Command Modes

CONFIGURATION

## Supported Modes

Full-Switch Mode

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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) snmp-server view rview 1.3.6.1 included
```

## Related Commands

[show running-config](#) — displays the SNMP running configuration.

# 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

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [show logging](#) — displays logging settings and system messages in the internal buffer.

### 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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [default 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

**Supported Modes** Full-Switch Mode



<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [logging console](#) — sets the logging console parameters.

## logging extended

Logs security and audit events to a system log server.

**Syntax** `logging extended`

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch 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
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.5(0.0)</b>	Introduced on the 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

## 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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode


Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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. You can configure multiple logging servers of both IPv4 and/or IPv6.

**Syntax** `logging {ip-address | ipv6-address | hostname} {{udp {port}} | {tcp {port}}}`  
 To disable logging, use the `no logging` command.

Parameters		
<b>ip-address</b>		Enter the IPv4 address in dotted decimal format.
<b>ipv6-address</b>		Enter the IPv6 address in the x:x:x::X format.  <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
<b>hostname</b>		Enter the name of a host already configured and recognized by the switch.
<b>udp</b>		Enter the keyword <code>udp</code> to enable transmission of log message over UDP followed by port number. The default port is 514
<b>tcp</b>		Enter the keyword <code>tcp</code> to enable transmission of log message over TCP followed by port number.

**Defaults** Disabled.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced <b>udp</b> and <b>tcp</b> keywords on the MXL 10/40GbE Switch.

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes**

Full-Switch Mode

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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)
- `local10` (local use)
- `local11` (local use)
- `local12` (local use)
- `local13` (local use)
- `local14` (local use)
- `local15` (local use)
- `local16` (local use)
- `local17` (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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 system 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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>logging source-interface <i>interface</i></code> To disable this command and return to the default setting, use the <code>no logging source-interface</code> command.						
<b>Parameters</b>	<p><b><i>interface</i></b> Enter the following keywords and slot/port or number information:</p> <ul style="list-style-type: none"><li>• For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383.</li><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a ten-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>						
<b>Defaults</b>	Not configured.						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	Syslog messages contain the IP address of the interface used to egress the router. By configuring the <code>logging source-interface</code> command, the Syslog packets contain the IP address of the interface configured.						
<b>Related Commands</b>	<a href="#">logging</a> — enables logging to the Syslog server.						

# logging synchronous

Synchronize unsolicited messages and output.

<b>Syntax</b>	<code>logging synchronous [level <i>level</i>   all] [limit <i>number-of-buffers</i>]</code> To disable message synchronization, use the <code>no logging synchronous [level <i>level</i>   all] [limit <i>number-of-buffers</i>]</code> command.
<b>Parameters</b>	<p><b>all</b> Enter the keyword <code>all</code> to ensure that all levels are printed asynchronously.</p> <p><b>level <i>level</i></b> 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 <b>2</b>.</p> <p><b>all</b> Enter the keyword <code>all</code> to turn off all.</p> <p><b>limit <i>number-of-buffers</i></b> Enter the keyword <code>limit</code> 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 <b>20</b>.</p>
<b>Defaults</b>	Disabled. If enabled without the <code>level</code> or <code>number-of-buffers</code> options specified, <code>level = 2</code> and <code>number-of-buffers = 20</code> are the defaults.
<b>Command Modes</b>	LINE
<b>Supported Modes</b>	Full-Switch Mode

<b>Command History</b>	<table border="0"> <tr> <td style="text-align: right;"><b>Version</b></td> <td>Description</td> </tr> <tr> <td style="text-align: right;"><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td style="text-align: right;"><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </table>	<b>Version</b>	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>When you enable <code>logging synchronous</code>, 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.</p> <p>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.</p>						
<b>Related Commands</b>	<a href="#">logging on</a> — enables logging.						

## logging trap

Specify which messages are logged to the Syslog server based the message severity.

<b>Syntax</b>	<code>logging trap [level]</code>						
	To return to the default values, use the <code>default logging trap</code> command.						
	To disable logging, use the <code>no logging trap</code> command.						
<b>Parameters</b>	<table border="0"> <tr> <td style="text-align: right;"><b>level</b></td> <td>Indicate a value from 0 to 7 or enter one of the following parameters: <code>emergencies</code>, <code>alerts</code>, <code>critical</code>, <code>errors</code>, <code>warnings</code>, <code>notifications</code>, <code>informational</code>, or <code>debugging</code>. The default is <b>6</b> or <b>informational</b>.</td> </tr> </table>	<b>level</b>	Indicate a value from 0 to 7 or enter one of the following parameters: <code>emergencies</code> , <code>alerts</code> , <code>critical</code> , <code>errors</code> , <code>warnings</code> , <code>notifications</code> , <code>informational</code> , or <code>debugging</code> . The default is <b>6</b> or <b>informational</b> .				
<b>level</b>	Indicate a value from 0 to 7 or enter one of the following parameters: <code>emergencies</code> , <code>alerts</code> , <code>critical</code> , <code>errors</code> , <code>warnings</code> , <code>notifications</code> , <code>informational</code> , or <code>debugging</code> . The default is <b>6</b> or <b>informational</b> .						
<b>Defaults</b>	<b>6</b> or <b>informational</b>						
<b>Command Modes</b>	CONFIGURATION						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table border="0"> <tr> <td style="text-align: right;"><b>Version</b></td> <td><b>Description</b></td> </tr> <tr> <td style="text-align: right;"><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td style="text-align: right;"><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<p><a href="#">logging</a> — enables the logging to another device.</p> <p><a href="#">logging on</a> — enables logging.</p>						

## logging version

Displays syslog messages in a RFC 3164 or RFC 5424 format.

<b>Syntax</b>	<code>logging version {0 1}</code>				
<b>Defaults</b>	0				
<b>Command Modes</b>	CONFIGURATION				
<b>Supported Modes</b>	Full-Switch Mode				
<b>Command History</b>	<p>This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.</p> <p>The following is a list of the Dell Networking OS version history for this command.</p> <table border="0"> <tr> <td style="text-align: right;"><b>Version</b></td> <td><b>Description</b></td> </tr> <tr> <td style="text-align: right;"><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>Version</b>	<b>Description</b>				
<b>9.9(0.0)</b>	Introduced on the FN IOM.				



Version	Description
9.5(0.0)	Introduced on the MXL.

### Usage Information

To display syslog messages in a RFC 3164 or RFC 5424 format, use the **log version** command in configuration mode. By default, the system log version is set to **0**.

The following describes the two supported log messages formats:

- 0 – Displays syslog messages format as described in RFC 3164, The BSD syslog Protocol
- 1 – Displays SYSLOG message format as described in RFC 5424, The Syslog Protocol

### Example

```
Dell(conf)#logging version ?
<0-1> Select syslog version (default = 0)
Dell(conf)#logging version 1
```

## show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

**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 `history` to view only information in the Syslog history table.
- reverse** (OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
- summary** (OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot. Slots \*7\* and \*8\* represent RPMs.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

### Example (Partial)

```
Dell#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 311 Messages Logged, Size (40960 bytes)
  Trap logging: level informational
    Logging to 172.16.1.162
    Logging to 10.10.10.4
    Logging to 10.1.2.4
    Logging to 172.31.1.4
    Logging to 133.33.33.4
May 22 10:21:10: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
10.11.68.22 )by admin
May 22 10:16:35: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
10.11.68.22 )by admin
May 22 09:39:12: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
```

```

10.11.68.22 )by admin
May 22 09:03:56: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
10.11.68.22 )by admin
May 22 09:01:51: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
10.11.68.22 )by admin
May 22 08:53:09: %STKUNIT0-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS:
Enable password authentication suc
cess on vty0 ( 10.11.68.22 )
May 22 08:53:04: %STKUNIT0-M:CP %SEC-5-LOGIN_SUCCESS: Login successful
for user admin on vty0
(10.11.68.22)
May 19 16:58:32: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty2
(10.11.68.22)
May 19 14:22:48: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty2 (
10.11.68.22 )by admin
May 19 12:05:43: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty2 (
10.11.68.22 )by admin
May 19 10:23:59: %STKUNIT0-M:CP %SYS-5-CONFIG_I: Configured from vty0 (
10.11.68.22 )by admin
May 19 10:23:58: %STKUNIT0-M:CP %SEC-5-LOGOUT: Exec
--More--

```

### Example (History)

```

Dell#show logging history
Syslog History Table: 1 maximum table entries,
saving level warnings or higher
SNMP notifications not Enabled
May 22 08:53:09: %STKUNIT0-M:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS:
Enable
password authentication success on vty0 ( 10.11.68.22 )
Dell#

```

## show logging driverlog stack-unit

Display the driver log for the specified stack member.

**Syntax** `show logging driverlog stack-unit unit#`

**Parameters** **stack-unit *unit#*** Enter the keywords `stack-unit` then the stack member ID of the switch for which you want to display the driver log. The range is from 0 to 1.

**defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module..

**Usage Information** This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

## show logging auditlog

Displays an audit log.

**Syntax** `show logging auditlog`

**Defaults** none

**Command Modes** EXEC

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.5(0.0)	Introduced on the MXL.

**Example**

```
Dell(conf)#show logging audit
```

**Related Commands** [clear logging auditlog](#) — clears audit log.

## terminal monitor

Configure the system to display messages on the monitor/terminal.

**Syntax** terminal monitor

To return to default settings, use the `terminal no monitor` command.

**defaults** Disabled.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [logging monitor](#) — sets the logging parameters on the monitor/terminal.

# Stacking Commands

Stacking is supported on the FN410S and FN410T cards with ports 9 and 10 as the stack ports. Stacking is limited to six Aggregators in the same or different chassis in a single stack.

Stacking provides a single point of management and NIC teaming for high availability and higher throughput. To configure an Aggregator stack, you must use the CLI.

The stacking commands are always available and operational. You can use the commands to pre-configure an Aggregator, so that the configuration settings are invoked when the Aggregator is attached to other Aggregator blades.

For more information about using the Aggregator stacking feature, see the *Stacking Aggregators* chapter in the Dell Networking OS Configuration Guide for the FN IOM.

You can use the following commands to manage a stack of Aggregator I/O modules:

- [power-cycle stack-unit](#)
- [reset stack-unit](#)
- [show system stack-ports](#)
- [show system stack-unit stack-group](#)
- [stack-unit iom-mode](#)

**NOTE:** The terms `stack-unit-id`, `unit-id`, `stack-unit-number`, `stack-number`, and `unit-number` mentioned in this chapter refers to the `stack-unit-number`.

## Topics:

- [power-cycle stack-unit](#)
- [redundancy disable-auto-reboot](#)
- [redundancy force-failover stack-unit](#)
- [reset stack-unit](#)
- [show redundancy](#)
- [show system stack-ports](#)
- [show system stack-unit iom-mode](#)
- [show system stack-unit stack-group](#)
- [stack-unit iom-mode](#)
- [stack-unit priority](#)
- [stack-unit provision](#)
- [stack-unit renumber](#)
- [track-stack-ports disable-all-links](#)

## power-cycle stack-unit

To hard reset any stack unit including master unit.

**Syntax** `power-cycle stack-unit unit-number`

**Parameter** **Unit number** The unit number ranges from 0 to 5.

**Defaults** None

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.6.(0.0)	Supported on the FN I/O Aggregator.
8.3.17.0	Supported on the M I/O Aggregator.

#### Usage Information

This command is supported on the M I/O, FN410S, and FN410T Aggregators.

This command is used to reset the stack-unit. The master unit can also be power cycled using this command.

## redundancy disable-auto-reboot

Prevent the switch stack management unit from rebooting if it fail.

**Syntax** `redundancy disable-auto-reboot stack-unit [0-5 | members]`  
 To return to the default, use the `no redundancy disable-auto-reboot stack-unit [0-5 | members]` command.

**Defaults** Disabled (the failed switch is automatically rebooted).

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

#### Usage Information

When the command is given as `redundancy disable-auto-reboot stack-unit`, it prevents the switch stack management unit and standby unit from rebooting if they fail.

When a particular unit number in the range from 0 to 5 is issued as part of the CLI, it prevents that particular unit from rebooting after failure.

When members are issued as part of the CLI, all the units part of the stack are prevented from rebooting after failure.

The unit does not reboot until it is manually rebooted.

#### Related Commands

[show redundancy](#) — displays the current redundancy status.

## redundancy force-failover stack-unit

Force the standby unit in the stack to become the management unit.

**Syntax** `redundancy force-failover stack-unit`

**Defaults** Not enabled.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

# reset stack-unit

Reset any designated stack member except the management unit (master unit).

**Syntax** `reset stack-unit 0-5 hard`

**Parameters**

- 0-5** Enter the stack member unit identifier of the stack member to reset.
- hard** Reset the stack unit if the unit is in a problem state.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** This command is supported on the M I/O, FN410S, and FN410T Aggregators

Resetting the management unit is not allowed and an error message displays if you try to do so. Resetting is a soft reboot, including flushing the forwarding tables.

You can run this command directly on the stack standby unit (Standby Master) to reset the standby. You cannot reset any other unit from the standby unit

## Example

```
Dell#show system brief
Stack MAC : 00:1e:c9:f1:00:9b
-- Stack Info --
Unit      UnitType      Status      ReqTyp      CurTyp      Version      Ports
-----
0         Management    online      I/O-Aggregator I/O-Aggregator 8-3-17-46 56
1         Standby       online      I/O-Aggregator I/O-Aggregator 8-3-17-46 56
2         Member        not present
3         Member        not present
4         Member        not present
5         Member        not present
Dell#
Dell#reset stack-unit 0 >>>Resetting master not allowed
% Error: Reset of master unit is not allowed.
Dell#
Dell#reset stack-unit 1
Dell#01:02:00: %STKUNIT0-M:CP %CHMGR-5-STACKUNIT_RESET: Stack unit 1 being reset
01:02:00: %STKUNIT0-M:CP %IFMGR-1-DEL_PORT: Removed port: Te 1/1-32,41-56
01:02:00: %STKUNIT0-M:CP %CHMGR-2-STACKUNIT_DOWN: Stack unit 1 down - reset
01:02:00: %STKUNIT1-S:CP %IFMGR-1-DEL_PORT: Removed port: Te 1/1-32,41-56
01:02:05: %I/O-Aggregator:0 %IFAGT-5-STACK_PORT_LINK_DOWN: Changed stack port
state to down: 0/10
01:02:11: %STKUNIT0-M:CP %POLLMGR-2-ALT_STACK_UNIT_STATE: Alternate Stack-unit is
not present
Dell#01:02:12: %STKUNIT0-M:CP %CHMGR-2-STACKUNIT_DOWN: Stack unit 1 down - card
removed
```

**Related Commands** [reload](#)— reboots the system.

# show redundancy

Display the current redundancy configuration (status of automatic reboot configuration on stack management unit).

**Syntax** `show redundancy`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show redundancy

-- Stack-unit Status --
-----
Mgmt ID:                0
Stack-unit ID:          0
Stack-unit Redundancy Role: Primary
Stack-unit State:       Active
Stack-unit SW Version:  E8-3-16-160
Link to Peer:           Down
Peer Stack-unit:        not present

-- Stack-unit Redundancy Configuration --
-----
Primary Stack-unit:     mgmt-id 0
Auto Data Sync:         Full
Failover Type:          Hot Failover
Auto reboot Stack-unit: Enabled
Auto failover limit:    3 times in 60 minutes

-- Stack-unit Failover Record --
-----
Failover Count:         0
Last failover timestamp: None
Last failover Reason:   None
Last failover type:     None

-- Last Data Block Sync Record: --
-----
Stack Unit Config:     no block sync done
  Start-up Config:     no block sync done
Runtime Event Log:     no block sync done
  Running Config:      no block sync done
  ACL Mgr:              no block sync done
    LACP:               no block sync done
    STP:                 no block sync done
    SPAN:                no block sync done

Dell#
```

## Related Commands

[redundancy disable-auto-reboot](#) — prevents the system from auto-rebooting if it fails.

# show system stack-ports

Display information about the stacking ports on all switches in the FN I/O Aggregator switch stack..

### Syntax

```
show system stack-ports [status | topology]
```

### Parameters

- |                 |  |
|-----------------|--|
| <b>status</b>   | (OPTIONAL) Enter the keyword <code>status</code> to display the command output without the Connection field.       |
| <b>topology</b> | (OPTIONAL) Enter the keyword <code>topology</code> to limit the table to just the Interface and Connection fields. |

### Defaults

none

### Command Modes

- EXEC
- EXEC Privilege

**Supported Modes** All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6.(0.0)	Supported on the FN I/O Aggregator.

## Usage Information

This command is supported on the M I/O, FN410S, and FN410T Aggregators.  
The following describes the `show interfaces` command shown in the following example.

Field	Description
<b>Topology</b>	Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone.
<b>Interface</b>	The unit/port ID of the connected stack port on this unit.
<b>Link Speed</b>	Link Speed of the stack port (10) in Gb/s.
<b>Admin Status</b>	The only currently listed status is Up.
<b>Connection</b>	The stack port ID to which this unit's stack port is connected.

## Example

```
Dell# show system stack-ports
Topology: Ring

Interface Connection Link Speed      Admin Link  Trunk
              (Gb/s)      Status Status  Group
0/9                10          up   down
0/10               1/10       10   up   up
1/9                10          up   down
1/10               0/10       10   up   up
Dell#
```

## Example (Status)

```
Dell# show system stack-ports status
Topology: Daisy chain
Interface Link Speed      Admin Link  Trunk
              (Gb/s)      Status Status  Group
0/9                10          up   down
0/10               10          up   up
1/9                10          up   down
1/10               10          up   up
```

## Example (Topology)

```
Dell# show system stack-ports topology
Topology: Daisy chain

Interface Connection Trunk
              Group

0/9
0/9          1/10
1/10
1/10         0/10
Dell        #
```

## Related Commands

[power-cycle stack-unit](#)—resets the designated stack member.  
[show diag](#)— displays the data plane or management plane input and output statistics of the designated component of the designated stack member.  
[show system](#)—displays the current status of all stack members or a specific member.



# show system stack-unit iom-mode

Displays the current iom-mode (stack/standalone) and the mode configured after next reboot.

**Syntax** `show system stack-unit unit-number iom-mode`

**Parameters** *unit number <0-5>* Enter the number of the member stack unit. The range is from 0 to 5.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage information** This command is supported on the M I/O, FN410S, and FN410T Aggregators

### Example

```
Dell#show system stack-unit all iom-mode ?
|
|           Pipe through a command
|
|<cr>
Dell#show system stack-unit all iom-mode
Unit      Boot-Mode      Next-Boot
-----
0          stack          stack
1          stack          stack
2          stack          stack
3          stack          stack
4          Not Present
5          Not Present
Dell#
```

# show system stack-unit stack-group

Displays the stack-groups present/configured for a FN I/O Aggregator stack unit.

**Syntax** `show system stack-unit unit-number stack-group [configured]`

**Parameters** *unit number <0-5>* Enter the number of the member stack unit. The range is from 0 to 5.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information** This command is supported on the M I/O, FN410S, and FN410T Aggregators.

### Example

```
Dell#show system stack-unit 0 stack-group ?
configured      Configured stack groups
```

```

| Pipe through a command
<cr>
Dell#show system stack-unit 0 stack-group configured
Configured stack groups in stack-unit 0
Dell#show system stack-unit 0 stack-group
Stack group Ports
-----
0          0/9
1          0/10
2          0/11
3          0/12
Dell#

```

**Related Commands**

[reload](#)— reboots the system.  
[show system](#)— displays the current status of all stack members or a specific member.

## stack-unit iom-mode

Toggle the operating mode between programmable multiplex, standalone, stack, full-switch, and VLT modes.

**Syntax** `stack-unit <unit-number> iom-mode [programmable-mux | stack | standalone | vlt | full-switch`

**Parameters**

- unit number** `<0-5>` Enter the number of the member stack unit. The range is from 0 to 5.
- programmable-mux** Enable programmable multiplex mode.
- stack** Enable stack mode.
- standalone** Enable stand-alone mode.
- vlt** Enable virtual link trunking mode.
- full-switch** Enable full-switch mode.

**Defaults** standalone

**Command Modes** • CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.6.(0.0)	Supported on the FN I/O Aggregator.
	8.3.17.0	Supported on the M I/O Aggregator.

**Usage Information** This command is supported on the M I/O, FN410S, and FN410T Aggregators.

**Example**

```

Dell(conf)#stack-unit 0 iom-mode stack
% You are about to stack your IOA module, please reload the IOA
and then plug in the stacking cable for the changes to take effect.
Dell(conf)#
Dell#

```

**Related Commands**

[reload](#)— Reboots the operating system.  
[show system](#)— displays the current status of all stack members or a specific member.

# stack-unit priority

Configure the ability of a switch to become the management unit of a stack.

**Syntax** `stack-unit stack-number priority 1-14`

**Parameters**

<b><i>stack-number</i></b>	Enter the stack member unit identifier.
<b><i>1-14</i></b>	This preference parameter allows you to specify the management priority of one backup switch over another, with 0 the lowest priority and 14 the highest. The switch with the highest priority value is chosen to become the management unit if the active management unit fails or on the next reload.

**Defaults** 0

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** This command is supported on the M I/O, FN410S, and FN410T Aggregators.

**Related Commands**

- [reload](#) – reboots Dell Networking Operating System (OS).
- [show system](#) – displays the status of all stack members or a specific member.

# stack-unit provision

Preconfigure a logical stacking ID of a switch that joins the stack. This is an optional command that is executed on the management unit.

**Syntax** `stack-unit 0-5] provision {MXL-10/40GbE}`

**Parameters**

<b><i>0-5</i></b>	Enter a stack member identifier, from 0 to 5, of the switch that you want to add to the stack.
<b><i>MXL-10/40GbE</i></b>	Enter the model identifier of the switch to be added as a stack member. This identifier is also referred to as the <i>provision type</i> .

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands**

- [reload](#) — reboots the system.
- [show system](#) — displays the status of all stack members or a specific member.

# stack-unit renumber

Change the stack member ID of any stack member or a stand-alone unit.

**Syntax** `stack-unit 0-5 renumber 0-5`

**Parameters**      **0-5**      The first instance of this value is the stack member unit identifier, from 0 to 5, of the switch that you want add to the stack. The range is from 0 to 5. The second instance of this value is the desired new unit identifier number.

**Defaults**      none

**Command Modes**      EXEC Privilege

**Supported Modes**      All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6.(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.3(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information**      This command is supported on the FN410S and the FN410T Aggregators.  
You can renumber any switch, including the management unit or a stand-alone unit.  
You cannot renumber a unit to a number of an active member in the stack.  
When executing this command on the master, the stack reloads. When the members are renumbered, only that specific unit is reset and comes up with the new unit number.

**Example**

```
Dell#stack-unit 5 renumber 4

Renumbering will reset the unit.
Warning: Interface configuration for current unit will be lost!
Proceed to renumber [confirm yes/no]:
```

- Related Commands**
- [reload](#) – reboots Dell Networking Operating System (OS).
  - [reset stack-unit](#) – resets the designated stack member.
  - [show system](#) – displays the current status of all stack members or a specific member.

## track-stack-ports disable-all-links

Disables or shuts down internal and external ports on the system if both the stack link on the unit fails.

**Syntax**      `track-stack-ports disable-all-links`


**Defaults**      Not configured

**Command Modes**      CONFIGURATION

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

<b>Version</b>	<b>Description</b>
<b>9.14.0.0</b>	Introduced on the FN-IOM.

**Usage Information**      This command enables the switch to detect when both stack links fail and shuts down all uplink (external) and downlink (internal) ports. If a single stack port on a system is down, this command does not shut down ports.

 **NOTE:** Dell EMC Networking recommends disabling UFD when you enable this feature.

Use this command in a stack set up with only three or less units to avoid stack split.

This command is available only in Stack mode of the FN-IOM.

**Example**

```
Dell(conf)#track-stack-ports disable-all-links
```

```
Warning: Enabling stack-port tracking shuts down all the operationally
UP interfaces, when both/all the stack ports of the unit are down.
This Action is not modified when enabled along with UFD feature.
Dell(conf)#Jul  8 09:05:23 %STKUNIT0-M:CP %IFMGR-5-STK_PORT_ADDED: Stack
ports are now tracked for link failure
```

```
Dell(conf)#no track-stack-ports disable-all-links
Dell(conf)#Jul  8 09:06:29 %STKUNIT0-M:CP %IFMGR-5-STK_PORT_CLEARED:
Stack ports are no longer tracked for link failure
```

# Storm Control

The Dell Networking operating software storm control feature allows you to limit or suppress traffic during a traffic storm.

## 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.
- i 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.
- i 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 0 drops` command.

### Topics:

- [io-aggregator broadcast storm-control](#)
- [show io-aggregator broadcast storm-control status](#)
- [show storm-control unknown-unicast](#)
- [show storm-control broadcast](#)
- [show storm-control multicast](#)
- [storm-control multicast \(Interface\)](#)
- [storm-control broadcast \(Configuration\)](#)
- [storm-control broadcast \(Interface\)](#)
- [storm-control multicast \(Configuration\)](#)
- [storm-control PFC/LLFC](#)
- [storm-control unknown-unicast \(Configuration\)](#)
- [storm-control unknown-unicast \(Interface\)](#)

## io-aggregator broadcast storm-control

Rate-limit the traffic storm to 1 Gbps.

**Syntax**                    `io-aggregator broadcast storm-control`

To disable storm control, use the `no io-aggregator broadcast storm-control` command.

**Defaults** Enabled

**Command Modes** • CONFIGURATION

**Supported Modes** Standalone-Mux (SMUX)  
Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

**Usage Information** This command is not available in PMUX mode.

## show io-aggregator broadcast storm-control status

Shows if storm control is enabled or disabled. If enabled, displays information on the rate limit value.

**Syntax** `show io-aggregator broadcast storm-control status`

**Command Modes** • EXEC Privilege

**Supported Modes** Standalone-Mux (SMUX)  
Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

### Example

```
Dell#show io-aggregator broadcast storm-control status
Storm-Control Enabled
Broadcast Traffic limited to 1000 Mbps
Dell#
```

## show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

**Syntax** `show storm-control unknown-unicast [interface]`

**Parameters** *interface* (OPTIONAL) Enter the following interface to display the interface specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults** none

**Command Modes** • EXEC  
• EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)

Full-Switch Mode

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

## 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 information.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell#show storm-control broadcast tengigabitethernet 3/8
Broadcast storm control configuration
Interface      Direction  Packets/Second
-----
TenGig 3/8    Ingress    1000
Dell#
```

## 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 information.

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch Mode



Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

#### Example

```
Dell#show storm-control multicast gigabitethernet 1/1
Multicast storm control configuration
Interface  Direction      Packets/Second
-----
Te 2/2      Ingress          5
Dell#
```

## storm-control multicast (Interface)

Configure the percentage of multicast traffic allowed on the interface.

**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*** Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

**Command Modes** INTERFACE (conf-if-interface-slot/port)

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

## 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** ***packets\_per\_second*** 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)

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**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.

**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*** 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)

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic.

**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*** 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)

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 PFC/LLFC

Shut down the port if it receives the PFC/LLFC frames more than the configured rate.

<b>Syntax</b>	<code>storm-control pfc-llfc [pps]in shutdown</code>	
<b>Parameters</b>	<b><i>pfc-llfc in</i></b>	Enter the keyword <i>pfc-llfc</i> to get the flow control traffic. The range is from 0 to 33554368 packets per second.
	<b>shutdown</b>	Enter the keyword <i>shutdown</i> to shut down the port when the rate exceeds.


**Defaults** none

**Command Modes** INTERFACE (conf-if-interface-slot/port)

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

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

Version	Description
9.9(0.0)	Supported on the FN IOM, FN I/O Aggregator, and M I/O Aggregator

**Usage Information**  **NOTE:** PFC/LLFC storm control enabled interfaces disable the interfaces if it receives continuous PFC/LLFC packets. It can be a result of a faulty NIC/Switch that sends spurious PFC/LLFC packets.

# storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed on the switch (ingress rate only).

**Syntax** `storm-control unknown-unicast [packets_per_second in]`  
To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second in]` command.

**Parameters** ***packets\_per\_second*** Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch Mode

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.

**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 the interface.

**Syntax** `storm-control unknown-unicast [packets_per_second in]`  
To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [packets_per_second in]` command.

**Parameters**      ***packets\_per\_second***      Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554431.

**Command Modes**      INTERFACE (conf-if-*interface-slot/port*)

**Supported Modes**      Programmable-Mux (PMUX)  
Full-Switch Mode

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Introduced on the M I/O Aggregator.

# SupportAssist

SupportAssist sends troubleshooting data securely to Dell. SupportAssist in this Dell EMC Networking OS release does not support automated email notification at the time of hardware fault alert, automatic case creation, automatic part dispatch, or reports. SupportAssist requires Dell EMC Networking OS 9.9(0.0) and SmartScripts 9.7 or later to be installed on the Dell EMC Networking device. For more information on SmartScripts, see *Dell EMC Networking Open Automation guide*.

**NOTE:** SupportAssist is enabled by default on the system. To disable SupportAssist, enter the `eula-consent support-assist reject` command in Global Configuration mode and save the configuration.

## Topics:

- [eula-consent](#)
- [support-assist](#)
- [support-assist activate](#)
- [support-assist activity](#)
- [SupportAssist Commands](#)
- [SupportAssist Activity Commands](#)
- [SupportAssist Company Commands](#)
- [SupportAssist Person Commands](#)
- [SupportAssist Server Commands](#)
- [show eula-consent](#)
- [show running-config](#)
- [show support-assist status](#)

## eula-consent

Accept or reject the end user license agreement (EULA).

<b>Syntax</b>	<code>eula-consent {support-assist} {accept   reject}</code>	
<b>Parameters</b>	<b>support-assist</b>	Enter the keywords <code>support-assist</code> to either accept or reject the EULA for the specified service.
	<b>accept</b>	Enter the keyword <code>accept</code> to accept the EULA for the specified service.
	<b>reject</b>	Enter the keyword <code>reject</code> to reject the EULA for the specified service.
<b>Defaults</b>	None	
<b>Command Modes</b>	CONFIGURATION	
<b>Command History</b>	This guide is platform-specific. For command information about other platforms, see the relevant <i>Dell EMC Networking OS Command Line Reference Guide</i> .	

Version	Description
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

- When you run the command, the system displays a message with the information directing to the URL for further information.
- Even before you accept or reject the EULA, the configuration data is sent to the default centrally deployed SupportAssist Server. If you reject the EULA, the configuration data is not transmitted to the SupportAssist server.
- If there is an existing SupportAssist configuration, the configuration is not removed and the feature is disabled.

## Example

Accept the EULA:

```
DelleMC(conf)# eula-consent support-assist accept
I accept the terms of the license agreement. You can reject
the license agreement by configuring this command
'eula-consent support-assist reject'.
```

By installing SupportAssist, you allow Dell to save your contact information (e.g. name, phone number and/or email address) which would be used to provide technical support for your Dell products and services. Dell may use the information for providing recommendations to improve your IT infrastructure.

Dell SupportAssist also collects and stores machine diagnostic information, which may include but is not limited to configuration information, user supplied contact information, names of data volumes, IP addresses, access control lists, diagnostics & performance information, network configuration information, host/server configuration & performance information and related data ("Collected Data") and transmits this information to Dell. By downloading SupportAssist and agreeing to be bound by these terms and the Dell end user license agreement, available at: [www.dell.com/aeula](http://www.dell.com/aeula), you agree to allow Dell to provide remote monitoring services of your IT environment and you give Dell the right to collect the Collected Data in accordance with Dells Privacy Policy, available at: [www.dell.com/privacypolicycountryspecific](http://www.dell.com/privacypolicycountryspecific), in order to enable the performance of all of the various functions of SupportAssist during your entitlement to receive related repair services from Dell,. You further agree to allow Dell to transmit and store the Collected Data from SupportAssist in accordance with these terms. You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dells affiliates, subcontractors or business partners. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Collected Data being transferred in connection with SupportAssist. If you are downloading SupportAssist on behalf of a company or other legal entity, you are further certifying to Dell that you have appropriate authority to provide this consent on behalf of that entity. If you do not consent to the collection, transmission and/or use of the Collected Data, you may not download, install or otherwise use SupportAssist.

Reject the EULA:

```
DelleMC(conf)#eula-consent support-assist reject
Aug 24 22:35:38: %STKUNIT1-M:CP %SUPPORT_ASSIST-6-SUPASSIST_EVT: Event
monitor service stopped
I do not accept the terms of the license agreement. The SupportAssist
feature has
been deactivated and can no longer be used.
To enable SupportAssist configurations, accept the terms of the license
agreement
by configuring this command 'eula-consent support-assist accept'.
DelleMC(conf)#
DelleMC(conf)#
Aug 24 22:35:49: %STKUNIT1-M:CP %SUPPORT_ASSIST-6-
SUPASSIST_PKG_UNINSTALLED: SupportAssist package uninstalled
DelleMC(conf)#
```

## Related Commands

- [support-assist](#) — moves to the SupportAssist Configuration mode.

# support-assist

Move to the SupportAssist configuration mode.

**Syntax** `support-assist`  
To remove all the configuration of the SupportAssist service, use the `no support-assist` command.

**Command Modes** CONFIGURATION

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** If you reject the EULA, the data is not transmitted to the SupportAssist server.

**Related Commands** • [eula-consent](#) — accept or reject the EULA.

# support-assist activate

Launch the configuration wizard that enables SupportAssist service and guides through a series of commands to configure SupportAssist.

**Syntax** `support-assist activate`

**Command Modes** CONFIGURATION

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** You are guided through a series of queries to configure SupportAssist. The generated commands are added to the running configuration, including the DNS resolve commands, if configured.

This command starts the configuration wizard for the SupportAssist. At any time, you can exit by entering Ctrl-C. If necessary, you can skip some data entry.

Once you exit the wizard, the Dell EMC Networking OS starts a full transfer.

# support-assist activity

Trigger an activity event immediately.

**Syntax** `support-assist activity {full-transfer | core-transfer} start now`

**Parameters**


<b>full-transfer</b>	Enter the keyword <code>full-transfer</code> to specify transfer of configuration, inventory, logs, and other information.
<b>core-transfer</b>	Enter the keyword <code>core-transfer</code> to specify transfer of core files.

**Command Modes** EXEC Privilege

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** Use the command to trigger the activity that enables transfer of information. You can choose a full transfer that includes all the details or core transfer that includes only the core files.

 **NOTE:** The full transfer includes the core files as well in the information sent. The core transfer does not send core files that are older than 30 days.

## SupportAssist Commands

Dell EMC Networking OS supports the following SupportAssist mode commands.

### activity

Move to the SupportAssist Activity mode for an activity. Allow the user to configure customized details for a specific activity.

**Syntax** `activity {activity-name}`

To remove all customized detail for a specific activity, use the `no activity {activity-name}` command.

**Parameters**

<b>activity-name</b>	Enter one of the following keywords:
----------------------	--------------------------------------

- Enter the keyword `full-transfer` to enable or disable full transfer. You can create a custom file to transfer the outputs from a set of show commands. By default, the full transfer runs once in every 30 days.
- Enter the keyword `core-transfer` to enable or disable core transfer.
- Enter the keyword `event-transfer` to enable or disable event transfer. You can create a custom file to monitor a set of events.

**Command Modes** SUPPORTASSIST

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



Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM. Introduced the <code>core-transfer</code> and <code>event-transfer</code> parameters.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

#### Usage Information

By default, each activity follows a set of default actions using a default schedule. Using this command, you can customize the set of actions and disable a certain activity.

## contact-company

Configure the contact information for the company.

**Syntax** `contact-company name {company-name} [company-next-name] ... [company-next-name]`

To remove the contact company information, use the `no contact-company` command.

#### Parameters

<b><i>company-name</i></b>	Enter the name for the company. If there are multiple words in the name, use optional additional fields.
<b><i>company-next-name</i></b>	(OPTIONAL) Enter the next components of the company name, up to 5 components are allowed.

**Command Modes** SUPPORTASSIST

#### Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

#### Usage Information

You can configure only one contact-company.

It is not possible to remove the components of the company name. The `no` form of the command removes the entire contact-company entry.

This command is optional for SupportAssist service configuration.

## contact-person

Configure the contact name for an individual.

**Syntax** `contact-person [first <first-name>] last <last-name>`

To remove the contact person and all their details, use the `no contact-person [first <first-name>] last <last-name>` command.

<b>Parameters</b>	<b><i>first-name</i></b>	(Optional) Enter the first name for the contact person. This is optional provided each contact person name is unique. To include a space, enter a space within double quotes.
	<b><i>last-name</i></b>	Enter the last name for the contact person. To include a space, enter a space within double quotes.

**Command Modes** SUPPORTASSIST

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

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** Each contact person must be unique by their name.  
 You can configure only one contact person.  
 It is not possible to remove the first name or last name. The no form of the command removes the entire contact-person entry.  
 This command is optional for SupportAssist service configuration.

## enable

Enable all activities and severs for the SupportAssist service.

**Syntax** `enable all`  
 To disable the SupportAssist activities temporarily, use the `no enable all` command.

**Parameters** **all** Enter the keyword `all` to enable all SupportAssist service activities.

**Defaults** Enabled or All Enabled

**Command Modes** SUPPORTASSIST

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

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## server

Configure the name of the remote SupportAssist Server and move to SupportAssist Server mode.

**Syntax** `server {default | server-name}`

To delete a server, use the `no server server-name` command.

**Parameters**

<b>default</b>	Enter the keyword <code>default</code> for the default server.
<b>server-name</b>	Enter the name of the custom server to which the logs would be transferred. To include a space, enter a space within double quotes.

**Defaults** Default server has URL `stor.g3.ph.dell.com`

**Command Modes** SUPPORTASSIST

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

### Usage Information

The `server-name` is used as a reference only and is not required to be used as part of a URL definition.

There is a reserved name of `default` for the default server at `stor.g3.ph.dell.com`. You can customize the defaults for this server by entering the `server default` command and use the custom commands.

You can configure one additional server.

## SupportAssist Activity Commands

Dell EMC Networking OS supports the following SupportAssist Activity mode commands.

### action-manifest get

Copy an action-manifest file for an activity to the system.

**Syntax** `action-manifest get tftp | ftp | flash <file-specification> <local-file-name>`

**Parameters**

<b>file-specification</b>	Enter the full file specification for the action-manifest file. For example: <ul style="list-style-type: none"><li>• <code>tftp://hostip/filepath</code></li><li>• <code>ftp://userid:password@hostip/filepath</code></li><li>• <code>scp://userid:password@hostip/filepath</code></li></ul>
<b>local-file-name</b>	Enter the name of the local action-manifest file, up to 32 characters long. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

**Command Modes** SUPPORTASSIST ACTIVITY FULL-TRANSFER  
SUPPORTASSIST ACTIVITY EVENT-TRANSFER

## Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

The remote file specification for full transfer includes the protocol that is used to copy the file from the remote system.

The default Manifest-file for full transfer includes records like alarms, logs, operational, and configuration data.

## Related Commands

- [action-manifest install](#) — configure the action-manifest to use for a specific activity.
- [action-manifest show](#) — view the list of action-manifest for a specific activity.
- [action-manifest remove](#) — remove the action-manifest file for an activity.

# action-manifest install

Configure action-manifest to transfer a set of customized records for full transfer and to monitor a set of specified events for event transfer.

## Syntax

```
action-manifest install {default | <local-file-name>}
```

To revert to the default action-manifest file, use the `action-manifest install default` command.

## Parameters

<b>default</b>	Enter the keyword <code>default</code> to revert back to the default set of actions for an activity.
<b>local-file-name</b>	Enter the name of the local action-manifest file. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

## Defaults

Default

## Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER  
SUPPORTASSIST ACTIVITY EVENT-TRANSFER

## Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

To replace the default action-manifest with a customized one, copy the action-manifest file to the system using the `action-manifest get` command and then use the `action-manifest install` command. To revert to the default action-manifest file, use the `action-manifest install default` command.

- Related Commands**
- [action-manifest get](#) — copy an action-manifest file for an activity to the system.
  - [action-manifest show](#) — view the list of action-manifest for a specific activity.
  - [action-manifest remove](#) — remove the action-manifest file for an activity.

## action-manifest remove

Remove the action-manifest file from Dell EMC Networking OS.

**Syntax** `action-manifest remove <local-file-name>`

**Parameters** **local-file-name** Enter the name of the local action-manifest file. Allowable characters are: a to z, A to Z, 0 to 9, -, \_, and space.

**Command Modes** SUPPORTASSIST ACTIVITY FULL-TRANSFER  
SUPPORTASSIST ACTIVITY EVENT-TRANSFER

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** To revert to the default action-manifest file, use the `action-manifest install` command. If necessary, you can then remove the custom action-manifest file.

- Related Commands**
- [action-manifest get](#) — copy an action-manifest file for an activity to the system.
  - [action-manifest install](#) — configure the action-manifest to use for a specific activity.
  - [action-manifest show](#) — view the list of action-manifest for a specific activity.

## action-manifest show

View the list of action-manifest for a specific activity.

**Syntax** `action-manifest show {all}`

**Parameters** **all** Enter the keyword `all` to view the entire list of action-manifests that are available for an activity.

**Command Modes** SUPPORTASSIST ACTIVITY FULL-TRANSFER  
SUPPORTASSIST ACTIVITY EVENT-TRANSFER

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.

Version	Description
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

#### Related Commands

- [action-manifest get](#) — copy an action-manifest file for an activity to the system.
- [action-manifest install](#) — configure the action-manifest to use for a specific activity.
- [action-manifest remove](#) — remove the action-manifest file for an activity.

## enable

Enable a specific SupportAssist activity.

#### Syntax

`enable`

To disable a particular SupportAssist activity, use the `no enable` command.

#### Defaults

Enabled

#### Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER  
 SUPPORTASSIST ACTIVITY CORE-TRANSFER  
 SUPPORTASSIST ACTIVITY EVENT-TRANSFER


#### Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

#### Usage Information

Enter the specific SupportAssist activity mode and then enable it.

 **NOTE:** By default, the full transfer includes the core files. When you disable the core transfer activity, the full transfer excludes the core files.

#### Related Commands

- [activity](#) — move user to the SupportAssist Activity mode for that activity.

## SupportAssist Company Commands

Dell EMC Networking OS supports the following SupportAssist Company mode commands.

### address

Configure the address information for the company.

#### Syntax

```
address [city company-city] [{province | region | state} name] [country
company-country] [{postalcode | zipcode} company-code]
```

To remove a portion of the company address information, use the `no address [city | province | region | state | country | postalcode | zipcode]` command. For example, to remove the city alone, use the `no address city` command.

To remove the complete company contact information, use the `no address` command.

## Parameters

<b>city</b> <i>company-city</i>	(OPTIONAL) Enter the keyword <code>city</code> then the city or town for the company site. To include a space, enter a space within double quotes.
<b>province   region   state</b> <i>name</i>	(OPTIONAL) Enter the keyword <code>province</code> , <code>region</code> or <code>state</code> then the name of province, region or state for the company site. To include a space, enter a space within double quotes.
<b>country</b> <i>company-country</i>	(OPTIONAL) Enter the keyword <code>country</code> then the country for the company site. To include a space, enter a space within double quotes.
<b>postalcode   zipcode</b> <i>company-code</i>	(OPTIONAL) Enter the keyword <code>postalcode</code> or <code>zipcode</code> then the postal code or zip code for the company site, as one string with no spaces.

**Command Modes** SUPPORTASSIST COMPANY

## Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

The optional parameters must be provided in the following order: `city state country postalcode`. If specified in a different order, the command returns an error as follows:

```
DellEMC(conf-supportassist-cmpy-test)# address city Minneapolis
postalcode 55344 country USA state Minnesota
                                     ^
% Error: Invalid input at "^" marker.
```

This command is optional for SupportAssist service configuration.

## Example

```
DellEMC(conf-supportassist-cmpy-test)# address city Minneapolis state
Minnesota country USA postalcode 55344
```

## street-address

Configure the street address information for the company.

## Syntax

```
street-address {address1} [address2]...[address8]
```

To remove the street address, use the `no street-address` command.

## Parameters

<b>address1</b>	Enter the street address for the company.
<b>address2..address8</b>	(OPTIONAL) Enter the street address of the company site. Up to 8 fields are allowed.

**Command Modes** SUPPORTASSIST COMPANY

## Command History

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** This command is optional for SupportAssist service configuration.

## territory

Configure the territory and set the coverage for the company site.

**Syntax** `territory company-territory`  
To remove the company territory information, use the `no territory` command.

**Parameters** **company-territory** Enter the territory name for the company. To include a space, enter a space within double quotes. Use three-letter country codes like USA, IND, FRA, GER and so on.

**Command Modes** SUPPORTASSIST COMPANY

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** This command is optional for SupportAssist service configuration.

## SupportAssist Person Commands

Dell EMC Networking OS supports the following SupportAssist Person mode commands.

### email-address

Configure the email addresses to reach the contact person.

**Syntax** `email-address primary email-address [alternate email-address]`  
To remove an email address, use the `no email-address` command. To remove the primary and the alternate email addresses, use the `no email-address primary` and `no email-address alternate` commands respectively.



<b>Parameters</b>	<b>primary <i>email-address</i></b>	Enter the keyword <code>primary</code> then the primary email address for the person.
	<b>alternate <i>email-address</i></b>	Enter the keyword <code>alternate</code> then the alternate email address for the person.

**Command Modes** SUPPORTASSIST PERSON

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

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** The email addresses must have the standard form of `<username>@<email system>` to be considered valid.

This command is optional for SupportAssist service configuration.

**Related Commands**

- [preferred-method](#) — configure the preferred method for contacting the person.

## phone

Configure phone numbers to reach the contact person.

**Syntax** `phone primary phone [alternate phone]`

To remove a phone number, use the `no phone` command. To remove the primary and alternate phone numbers, use the `no phone primary` and `no phone alternate` commands respectively.

<b>Parameters</b>	<b>primary <i>phone</i></b>	Enter the keyword <code>primary</code> then the primary phone number for the person.
	<b>alternate <i>phone</i></b>	Enter the keyword <code>alternate</code> then the alternate phone number for the person.

**Command Modes** SUPPORTASSIST PERSON

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

<b>Version</b>	<b>Description</b>
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Usage Information** The phone numbers may contain country codes, area codes and extensions, if necessary. Allowable characters are 0 to 9, x, (, ), - and +.

This command is optional for SupportAssist service configuration.

## Related Commands

- [preferred-method](#) — configure the preferred method for contacting the person.

# preferred-method

Configure the preferred method for contacting the person.

**Syntax** `preferred-method {email | no-contact | phone}`

**Parameters**

<b>email</b>	Enter the keyword <code>email</code> to specify email as preferred method.
<b>no-contact</b>	Enter the keywords <code>no-contact</code> to specify that there is no preferred method.
<b>phone</b>	Enter the keyword <code>phone</code> to specify phone as preferred method.

**Defaults** `no-contact`

**Command Modes** `SUPPORTASSIST PERSON`

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

Version	Description
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Related Commands

- [email-address](#) — configure email addresses to reach the contact person.
- [phone](#) — configure phone numbers to reach the contact person.

# time-zone

Configure the time zone for contacting the person.

**Syntax** `time-zone zone +-HH:MM[start-time HH:MM] [end-time HH:MM]`

To remove the time zone, use the `no time-zone [zone | start-time | end-time]` command.

**Parameters**

<b>zone +-HH:MM</b>	Enter the keyword <code>zone</code> then a time difference from GMT expressed as HH:MM. This number may be preceded by either a + or – sign.
<b>start-time HH:MM</b>	Enter the keywords <code>start-time</code> then a starting time expressed as HH:MM. Use the 24-hour clock format.
<b>stop-time HH:MM</b>	Enter the keywords <code>stop-time</code> then a stopping time expressed as HH:MM. Use the 24-hour clock format.

**Command Modes** `SUPPORTASSIST PERSON`

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

Version	Description
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.

Version	Description
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

### Usage Information

This command is optional for SupportAssist service configuration.

## SupportAssist Server Commands

Dell EMC Networking OS supports the following SupportAssist Server mode commands.

### proxy-ip-address

Configure a proxy for reaching the SupportAssist remote server.

**Syntax** `proxy-ip-address {ipv4-address | ipv6-address} port port-number [ username userid password [ encryption-type] password ]`

To remove the proxy, use the `no proxy-ip-address` command.

### Parameters

<b>ipv4-address</b>	Enter the IP address of the proxy server in a dotted decimal format (A.B.C.D).
<b>ipv6-address</b>	Enter the IPv6 address of the proxy server in the x:x:x:x format. <i>i</i> <b>NOTE:</b> The :: notation specifies successive hexadecimal fields of zeros.
	<i>i</i> <b>NOTE:</b> To use the IPv6 address, the Open Automation package should also support IPv6 communications. For this purpose, SupportAssist requires Dell EMC Networking Open Automation 9.10(0.0) package or later.
<b>port port-number</b>	Enter the keyword <code>port</code> then the TCP/IP port number. The port number range is from 1024 to 65534.
<b>username userid</b>	(OPTIONAL) Enter the keyword <code>username</code> then the user ID used for the proxy server.
<b>password</b>	Enter the keyword <code>password</code> then the encryption-type or the user password.
<b>encryption-type</b>	(OPTIONAL) Enter an encryption type for the <code>password</code> you enter. <ul style="list-style-type: none"> <li>0 directs the system to interpret the password as clear text.</li> <li>7 indicates that the password is encrypted using a DES hashing algorithm.</li> </ul>
<b>password</b>	Enter a string up to 32 characters long.

**Defaults** encryption-type for the password is 0.

**Command Modes** SUPPORTASSIST SERVER

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

The passwords are stored encrypted in the running configuration.

## enable

Enable communication with the SupportAssist server.

**Syntax** `enable`

To disable communication to a specific SupportAssist server, use the `no enable` command.

**Defaults** Enabled

**Command Modes** SUPPORTASSIST SERVER

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Related Commands

- `server` — configure the name of the remote SupportAssist server.

## url

Configure the URL to reach the SupportAssist remote server.


**Syntax** `url uniform-resource-locator`

To delete the URL for the server, use the `no url` command.

## Parameters

**uniform-resource-locator** Enter a text string for the URL using one of the following formats:

- `http://[username:password@]<hostip>:<portNum>/<filepath>`
- `https://[username:password@]<hostip>:<portNum>/<filepath>`

 **NOTE:** The host IP for the server may be specified as an IPv4 address, an IPv6 address or as a DNS hostname. If using the DNS hostname, the DNS resolver will need to be configured and enabled.

**Command Modes** SUPPORTASSIST SERVER

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Usage Information

The URL should be formatted to follow the ISO format.

# show eula-consent

Display the EULA for the feature.

**Syntax** `show eula-consent {support-assist | other feature}`

**Parameters** **support-assist | other feature** Enter the keywords `support-assist` or the text corresponding to other feature.

**Command Modes** EXEC Privilege

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

## Example

```
DellEMC# show eula-consent support-assist

SupportAssist EULA has been: Accepted

Additional information about the SupportAssist EULA is as follows:

By installing SupportAssist, you allow Dell to save your contact
information
(e.g. name, phone number and/or email address) which would be used to
provide
technical support for your Dell products and services. Dell may use the
information
for providing recommendations to improve your IT infrastructure.

Dell SupportAssist also collects and stores machine diagnostic
information, which
may include but is not limited to configuration information, user
supplied contact
information, names of data volumes, IP addresses, access control lists,
diagnostics &
performance information, network configuration information, host/server
configuration
& performance information and related data (Collected Data) and
transmits this
information to Dell. By downloading SupportAssist and agreeing to be
bound by these
terms and the Dell end user license agreement, available at:
www.dell.com/aeula,
you agree to allow Dell to provide remote monitoring services of your IT
environment
and you give Dell the right to collect the Collected Data in accordance
with Dells
Privacy Policy, available at: www.dell.com/privacypolicycountryspecific,
in order to
enable the performance of all of the various functions of SupportAssist
during your
entitlement to receive related repair services from Dell,. You further
agree to
```

```

allow Dell to transmit and store the Collected Data from SupportAssist
in accordance
with these terms. You agree that the provision of SupportAssist may
involve
international transfers of data from you to Dell and/or to Dells
affiliates,
subcontractors or business partners. When making such transfers, Dell
shall ensure
appropriate protection is in place to safeguard the Collected Data being
transferred
in connection with SupportAssist. If you are downloading SupportAssist
on behalf
of a company or other legal entity, you are further certifying to Dell
that you
have appropriate authority to provide this consent on behalf of that
entity. If you
do not consent to the collection, transmission and/or use of the
Collected Data,
you may not download, install or otherwise use SupportAssist.
DellEMC#

```

## show running-config

Display the current configuration and changes from the default values.

**Syntax** `show running-config support-assist`

**Parameters** **support-assist** Enter the keyword `support-assist` to view the detailed configuration for the feature.

**Command Modes** EXEC Privilege

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

Version	Description
<b>9.11(0.0)</b>	Introduced on the M I/O Aggregator and FN IOM.
<b>9.10(0.1)</b>	Introduced on the S6010-ON and S4048T-ON.
<b>9.10(0.0)</b>	Introduced on the S3148.
<b>9.10(0.0)</b>	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
<b>9.9(0.0)</b>	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

### Example

```

DellEMC# show running-config support-assist
!
support-assist
enable all
!
activity event-transfer
  enable
  action-manifest install default
!
activity core-transfer
  enable
!
contact-company name Dell
  street-address F lane , Sector 30
  address city Brussels state HeadState country Belgium postalcode S328J3
!
contact-person first Fred last Nash
  email-address primary des@sed.com alternate sed@dol.com
  phone primary 123422 alternate 8395729

```

```

preferred-method email
time-zone zone +05:30 start-time 12:23 end-time 15:23
!
server Dell
  enable
  url http://1.1.1.1:1332
DellEMC#

```

## show support-assist status

Display information on SupportAssist feature status including any activities, status of communication, last time communication sent, and so on.

**Syntax** `show support-assist status`

**Command Modes** EXEC Privilege

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

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

### Example

```

DellEMC#show support-assist status
SupportAssist Service: Installed
EULA: Accepted
Server: default
  Enabled: Yes
  URL: https://stor.g3.ph.dell.com
Server: Dell
  Enabled: Yes
  URL: http://1.1.1.1:1332
Service status: Enabled

```

Activity	State	Last Start	Last Success
core-transfer 2016 09:43:56 IST	Success	Feb 15 2016 09:43:41 IST	Feb 15
event-transfer 2016 09:48:21 IST	Success	Feb 15 2016 09:47:43 IST	Feb 15
full-transfer 2016 09:38:27 IST	Success	Feb 15 2016 09:36:12 IST	Feb 15

```

DellEMC#

```

# Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP).

## Topics:

- [bridge-priority](#)
- [debug spanning-tree](#)
- [description](#)
- [disable](#)
- [forward-delay](#)
- [hello-time](#)
- [max-age](#)
- [portfast bpdupfilter default](#)
- [protocol spanning-tree](#)
- [show config](#)
- [show spanning-tree 0](#)
- [spanning-tree 0](#)

## 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**

<b><i>priority-value</i></b>	Enter a number as the bridge priority value. The range is from 0 to 65535. The default is <b>32768</b> .
<b>primary</b>	Enter the keyword <code>primary</code> to designate the bridge as the root bridge.
<b>secondary</b>	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".)

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

**Syntax** `debug spanning-tree {stp-id [all | bpdu | events | exceptions] | protocol}`  
To disable debugging, use the `no debug spanning-tree` command.

**Parameters**

<b><i>stp-id</i></b>	Enter zero (0). The switch supports one spanning tree group with a group ID of 0.
----------------------	---



<b><i>protocol</i></b>	Enter the keyword for the type of STP to debug, either <code>mstp</code> , <code>pvst</code> , or <code>rstp</code> .
<b>all</b>	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
<b>bpdu</b>	(OPTIONAL) Enter the keyword <code>bpdu</code> to debug bridge protocol data units.
<b>events</b>	(OPTIONAL) Enter the keyword <code>events</code> to debug STP events.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

**Related Commands** [portfast bpdupfilter default](#) — 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”.)

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [portfast bpdupfilter default](#) — 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

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
------------------------	----------------	-------------

<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Related Commands** [portfast bpdupfilter default](#) — enters SPANNING TREE mode.

## 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 that the system waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is **15 seconds**.

**Defaults** **15 seconds**

**Command Modes** SPANNING TREE

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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** `hello-time seconds`  
To return to the default value, use the `no hello-time` command.

**Parameters** **seconds** Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

**Defaults** **2 seconds**

**Command Modes** SPANNING TREE

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>max-age seconds</code> To return to the default values, use the <code>no max-age</code> command.						
<b>Parameters</b>	<b>seconds</b> Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is <b>20 seconds</b> .						
<b>Defaults</b>	<b>20 seconds</b>						
<b>Command Modes</b>	SPANNING TREE						
<b>Supported Modes</b>	Full-Switch Mode						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Related Commands</b>	<a href="#">forward-delay</a> — changes the wait time before STP transitions to the Forwarding state. <a href="#">hello-time</a> — changes the time interval between BPDUs.						

# portfast bpdufilter default

Enable BPDU Filter globally to filter transmission of BPDU on port fast enabled interfaces.

<b>Syntax</b>	<code>portfast bpdufilter default</code> To disable global bpdu filter default, use the <code>no edge-port bpdufilter default</code> command.						
<b>Defaults</b>	Disabled						
<b>Command Modes</b>	SPANNING TREE						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN MXL.</td></tr><tr><td><b>8.3.16.1</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN MXL.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN MXL.						
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

# protocol spanning-tree

To enable and configure the spanning tree group, enter SPANNING TREE mode.

<b>Syntax</b>	<code>protocol spanning-tree stp-id</code> To disable the Spanning Tree group, use the <code>no protocol spanning-tree stp-id</code> command.				
<b>Parameters</b>	<b>stp-id</b> Enter zero (0). The system supports one spanning tree group, group 0.				
<b>Defaults</b>	Not configured.				
<b>Command Modes</b>	CONFIGURATION				
<b>Supported Modes</b>	Full-Switch Mode				
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.
Version	Description				
<b>9.9(0.0)</b>	Introduced on the FN IOM.				

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the `no disable` command from SPANNING TREE mode.

**Example**

```
Dell(conf)#protocol spanning-tree 0
Dell(config-stp)#
```

**Related Commands**

`disable` — disables spanning tree group 0. To enable spanning tree group 0, use the `no disable` command.

## show config

Display the current configuration for the mode. Only non-default values display.

**Syntax** `show config`

**Command Modes** SPANNING TREE

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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	
<b>0</b>	Enter 0 (zero) to display information about that specific spanning tree group.
<b>active</b>	(OPTIONAL) Enter the keyword <code>active</code> to display only active interfaces in spanning tree group 0.
<b>brief</b>	(OPTIONAL) Enter the keyword <code>brief</code> to display a synopsis of the spanning tree group configuration information.
<b>guard</b>	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an STP interface and the current port state.
<b>interface <i>interface</i></b>	(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: <ul style="list-style-type: none"><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li></ul>
<b>root</b>	(OPTIONAL) Enter the keyword <code>root</code> to display configuration information on the spanning tree group root.

**summary** (OPTIONAL) Enter the keyword `summary` to only the number of ports in the spanning tree group and their state.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch Mode

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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
<b>“Bridge Identifier...”</b>	Lists the bridge priority and the MAC address for this STP bridge.
<b>“Configured hello...”</b>	Displays the settings for hello time, max age, and forward delay.
<b>“We are...”</b>	States whether this bridge is the root bridge for the STG.
<b>“Current root...”</b>	Lists the bridge priority and MAC address for the root bridge.
<b>“Topology flag...”</b>	States whether the topology flag and the detected flag were set.
<b>“Number of...”</b>	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
<b>“Timers”</b>	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
<b>“Times”</b>	List the number of seconds since the last: <ul style="list-style-type: none"><li>• hello time</li><li>• topology change</li><li>• notification</li><li>• aging</li></ul>
<b>“Port 1...”</b>	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
<b>“Port path...”</b>	Displays the path cost, priority, and identifier for the interface.
<b>“Designated root...”</b>	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.
<b>“Designated port...”</b>	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 2 (TenGigabitEthernet 1/1) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.26
```

```

Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.26, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 3 (TenGigabitEthernet 1/2) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.27
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.27, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:18, received 0
The port is not in the portfast mode

Port 4 (TenGigabitEthernet 1/3) is Forwarding
Port path cost 4, Port priority 8, Port Identifier 8.28
Designated root has priority 32768, address 0001.e800.0a56
Designated bridge has priority 32768, address 0001.e800.0a56
Designated port id is 8.28, designated path cost 0
Timers: message age 0, forward_delay 0, hold 0
Number of transitions to forwarding state 1
BPDU: sent:31, received 0
The port is not in the portfast mode

Dell#

```

### Example (Brief)

#### Usage Information

The following describes the `show spanning-tree 0 guard` command shown in the example.

Field	Description
<b>Interface Name</b>	STP interface.
<b>Instance</b>	STP 0 instance.
<b>Sts</b>	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
<b>Guard Type</b>	Type of STP guard configured (Root, Loop, or BPDU guard).
<b>Bpdu Filter</b>	BPDU Filter enabled - Yes, BPDU Filter disabled - No

### Example (Guard)

```

Dell#show spanning-tree 0 guard
Interface
Name      Instance Sts          Guard type
-----
Te 0/1 0      INCON(Root)  Rootguard
Te 0/2 0      LIS          Loopguard
Te 0/3 0      EDS (Shut)   Bpduguard

```

## spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

#### Syntax

```
spanning-tree stp-id {cost cost | {rootguard} | portfast [bpduguard
[shutdown-on-violation] | bpdufilter] | priority priority}
```

To disable Spanning Tree group on an interface, use the `no spanning-tree stp-id {cost cost | {rootguard} | portfast [bpduguard [shutdown-on-violation] | bpdufilter] | priority priority}` command.

<b>Parameters</b>	<b><i>stp-id</i></b>	Enter the STP instance ID. The range is 0.
	<b><i>cost cost</i></b>	Enter the keyword <code>cost</code> then a number as the cost. The range is 1 to 65535. The defaults are: <ul style="list-style-type: none"> <li>• 10-Gigabit Ethernet interface = <b>2</b>.</li> <li>• Port Channel interface with 10-Gigabit Ethernet = <b>1</b>.</li> </ul>
	<b><i>rootguard</i></b>	Enter the keyword <code>rootguard</code> to enable STP root guard on a port or port-channel interface.
	<b><i>portfast</i> <b>[<i>bpduguard</i> <i>shutdown-on-violation</i>]   <i>bpdufilter</i></b></b>	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 keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.  Enter the keyword <code>bpdufilter</code> to enable on an interface; it should stop sending and receiving BPDUs on the port fast enabled ports.
	<b><i>priority priority</i></b>	Enter keyword <code>priority</code> then a number as the priority. The range is zero (0) to 15. The default is <b>8</b> .

**Defaults** cost = depends on the interface type; priority = **8**

**Command Modes** INTERFACE

**Supported Modes** Full-Switch Mode

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module..

**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 still are sent to the RPM CPU.

STP root guard is 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.

# System Time

The commands in this chapter configure time values on the system, either using the Dell Networking OS, 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 NTP commands are:

- [show clock](#)
- [clock set](#)
- [clock summer-time date](#)
- [clock summer-time recurring](#)

## Topics:

- [clock set](#)
- [clock summer-time date](#)
- [clock summer-time recurring](#)
- [debug ntp](#)
- [ntp offset-threshold](#)
- [ntp server](#)
- [ntp authenticate](#)
- [ntp authentication-key](#)
- [ntp control-key-passwd](#)
- [ntp master <stratum>](#)
- [ntp server](#)
- [ntp source](#)
- [ntp trusted-key](#)
- [show clock](#)
- [show ntp associations](#)
- [show ntp vrf associations](#)
- [show ntp status](#)

## clock set

Set the software clock in the switch.

**Syntax** `clock set time month day year`

<b>Parameters</b>	<b><i>time</i></b>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
	<b><i>month</i></b>	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to <i>time day month year</i> .
	<b><i>day</i></b>	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 <i>time month day year</i> .
	<b><i>year</i></b>	Enter a four-digit number as the year. The range is from 1993 to 2035.

**Defaults** Not configured.

**Command Modes** EXEC Privilege

**Supported Modes** All Modes



<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	<p>You can change the order of the <code>month</code> and <code>day</code> parameters to enter the time and date as <code>time day month year</code> . You cannot delete the software clock.</p> <p>The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.</p> <p>Dell Networking recommends using an outside time source, such as NTP, to ensure accurate time on the switch.</p>	
<b>Example</b>	<pre>Dell#clock set 12:11:00 21 may 2012 Dell#</pre>	

## 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.

<b>Parameters</b>	<b><i>time-zone</i></b>	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
	<b><i>start-month</i></b>	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 <code>time day month year</code> .
	<b><i>start-day</i></b>	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 <code>time day month year</code> .
	<b><i>start-year</i></b>	Enter a four-digit number as the year. The range is from 1993 to 2035.
	<b><i>start-time</i></b>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
	<b><i>end-day</i></b>	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 <code>time day month year</code> .
	<b><i>end-month</i></b>	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 <code>time day month year</code> .
	<b><i>end-time</i></b>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
	<b><i>end-year</i></b>	Enter a four-digit number as the year. The range is from 1993 to 2035.
	<b><i>offset</i></b>	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is <b>60 minutes</b> .

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## 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

<b><i>time-zone</i></b>	Enter the three-letter name for the time zone. This name is displayed in the <code>show clock</code> output. You can enter up to eight characters.
<b><i>start-week</i></b>	(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for <i>start-day</i> through <i>end-time</i> : <ul style="list-style-type: none"><li>• <i>week-number</i>: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time.</li><li>• <i>first</i>: Enter this keyword to start daylight saving time in the first week of the month.</li><li>• <i>last</i>: Enter this keyword to start daylight saving time in the last week of the month.</li></ul>
<b><i>start-day</i></b>	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.
<b><i>start-month</i></b>	Enter the name of one of the 12 months in English.
<b><i>start-time</i></b>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<b><i>end-week</i></b>	Enter the one of the following as the week that daylight saving ends: <ul style="list-style-type: none"><li>• <i>week-number</i>: enter a number from 1 to 4 as the number of the week to end daylight saving time.</li><li>• <i>first</i>: enter the keyword <i>first</i> to end daylight saving time in the first week of the month.</li><li>• <i>last</i>: enter the keyword <i>last</i> to end daylight saving time in the last week of the month.</li></ul>
<b><i>end-day</i></b>	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.
<b><i>end-month</i></b>	Enter the name of one of the 12 months in English.
<b><i>end-time</i></b>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
<b><i>offset</i></b>	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is <b>60 minutes</b> .

## Defaults

Not configured.

## Command Modes

CONFIGURATION

## Supported Modes

All Modes

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

Version	Description
8.3.17.0	Supported on the M I/O Aggregator.

**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.

## debug ntp

Display network time protocol (NTP) transactions and protocol messages for troubleshooting.

**Syntax** `debug ntp {level level-number}`

To disable debugging of NTP transactions, use the `no debug ntp {level level-number}` command.

**Parameters** **level level-number** Enter the keyword `level` then the `level-number` to display information about NTP logs. The log level range is from 1 to 6.

- 1 is the most important log level.
- 6 is the least important log level.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.14(0.0)	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON, and Z9100-ON.

## ntp offset-threshold

Configure the threshold time interval before which the system generates an NTP audit log message if the time difference from the NTP server is greater than a threshold value (`offset-threshold`).

**Syntax** `ntp offset-threshold threshold-value`

To disable the threshold value, use the `no ntp offset-threshold` command.

**Parameters** **offset-threshold threshold-value** (Optional) Enter the keyword `offset-threshold` and then the threshold value. The range is from 0 to 999.

**Defaults** Zero (0).

**Command Modes** CONFIGURATION

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

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S3038-ON, S4048-ON, S3100 Series, S4810P, S4820T, S5000, S6000, S6000-ON, S6100-ON, Z9500, and Z9100-ON.

**Usage Information** The `ntp offset-threshold` command does not time synchronization.

## Example

```
DellEMC(config)# ntp offset-threshold 4
```

# ntp server

Configure an NTP time-serving host.

**Syntax** `ntp server {ipv4-address}`

**Parameters** *ipv4-address* Enter an IPv4 address (A.B.C.D).

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Usage Information** You can configure multiple time-serving hosts (up to 250). From these time-serving hosts, the operating system chooses one NTP host with which to synchronize.

Because many polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.

# 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You also must configure an authentication key for NTP traffic using the `ntp authentication-key` command.

**Related Commands** [ntp authentication-key](#) — configures the authentication key for NTP traffic.  
[ntp trusted-key](#) — configures a key to authenticate.

# ntp authentication-key

Specify a key for authenticating the NTP server.

**Syntax** `ntp authentication-key number md5 [0 | 7] key`

<b>Parameters</b>	<p><b><i>number</i></b> Specify a number for the authentication key. The range is from 1 to 65534. This number must be the same as the <code>number</code> parameter configured in the <code>ntp trusted-key</code> command.</p> <p><b><i>md5</i></b> Specify that the authentication key is encrypted using MD5 encryption algorithm.</p> <p><b><i>0</i></b> Specify that authentication key is entered in an unencrypted format (default).</p> <p><b><i>7</i></b> Specify that the authentication key is entered in DES encrypted format.</p> <p><b><i>key</i></b> Enter the authentication key in the previously specified format.</p>								
<b>Defaults</b>	NTP authentication is not configured by default. If you do not specify the option [0   7], <b>0</b> is selected by default.								
<b>Command Modes</b>	CONFIGURATION								
<b>Supported Modes</b>	Full-Switch								
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;">Description</th> </tr> </thead> <tbody> <tr> <td><b>9.14(0.0)</b></td> <td>The trusted-key range value is increased from 1 to 65534.</td> </tr> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>8.3.16.1</b></td> <td>Introduced on the MXL 10/40GbE Switch IO Module.</td> </tr> </tbody> </table>	<b>Version</b>	Description	<b>9.14(0.0)</b>	The trusted-key range value is increased from 1 to 65534.	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Version</b>	Description								
<b>9.14(0.0)</b>	The trusted-key range value is increased from 1 to 65534.								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.								
<b>Usage Information</b>	<p>After configuring the <code>ntp authentication-key</code> command, configure the <code>ntp trusted-key</code> command to complete NTP authentication.</p> <p>The Dell Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous versions; beginning in version 8.2.1.0, the system uses DES encryption to store the key in the startup-config when you enter the <code>ntp authentication-key</code> command. Therefore, if your system boots with a startup-configuration from an versions prior to 8.2.1.0 in which you have configured <code>ntp authentication-key</code>, 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.</p>								
<b>Related Commands</b>	<p><a href="#">ntp authenticate</a> — enables NTP authentication.</p> <p><a href="#">ntp trusted-key</a> — configures a trusted key.</p>								

## ntp control-key-passwd

Configure control key password for NTPQ authentication. NTP control key supports encrypted and unencrypted option.

**Syntax** `ntp control-key-passwd [encryption-type] password`

To delete the control key, use the `no ntp control-key-passwd [encryption-type] password` command.

**Parameters**

***encryption-type*** (OPTIONAL) Enter one of the following numbers:

- 0 (zero) for an unencrypted (clear text) password
- 7 (seven) for a hidden text or DES encrypted

***password*** Enter a string up to 32 characters as the password.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

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

Version	Description
9.14(0.0)	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048-ON, S4048-ON, S4048T-ON, S5048F-ON, S6000, S6000-ON, S6010-ON, S6100-ON, and Z9100-ON.

**Usage Information**

NTP control key is not configured by default. If the encryption-type (0 or 7) is not specified, then 0 is selected by default.

**Related Commands**

- [ntp authentication-key](#)—sets an authentication key for NTP.
- [ntp authenticate](#)—enables the NTP authentication parameters that you set.
- [ntp server](#)—configures an NTP time-serving host.

## ntp master <stratum>

Configure the switch as NTP Server.

**Syntax** `ntp master <stratum>`

**Parameters** **ntp master <stratum>** Enter the keyword `stratum` number to identify the NTP Server's hierarchy. The `stratum` range value is from 2 to 15 and the default value is 8.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.6(0.0)	Introduced on the MXL.

## ntp server

Configure an NTP time-serving host.

**Syntax** `ntp server[vrf vrf-name] {hostname | ipv4-address | ipv6-address} [key keyid] [prefer] [version number] [minpoll] [maxpoll]`

**Parameters**

- vrf vrf-name** (Optional) Enter the keyword `vrf` and then the name of the VRF to configure a NTP time-serving host corresponding to that VRF.
- ipv4-address | ipv6-address** Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X) of NTP server.
- hostname** Enter the hostname of the server.
- key keyid** (OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. The range is from 1 to 65534.
- prefer** (OPTIONAL) Enter the keyword `prefer` to indicate that this peer has priority over other servers.
- version number** (OPTIONAL) Enter the keyword `version` and a number to correspond to the NTP version used on the server. The range is from 1 to 4.
- minpoll polling-interval** (OPTIONAL) Enter the keyword `minpoll` then the polling-interval. The polling interval range is from 4 to 16.

**maxpoll polling-interval** (OPTIONAL) Enter the keyword `maxpoll` then the polling-interval. The polling interval range is from 4 to 16.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.14(0.0)</b>	The trusted-key range value is increased from 1 to 65534. Also, introduced the <code>minpoll</code> and <code>maxpoll</code> polling interval options.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Added support for VRF.
	<b>8.3.11.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** You can configure multiple time-serving hosts (up to 250). From these time-serving hosts, the system 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 OS 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 Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `lag` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For the Management interface, enter the keyword `ManagementEthernet` then slot/port information. This option is valid only in Full-Switch mode.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# ntp trusted-key

Set a key to authenticate the system to which NTP synchronizes.

**Syntax** `ntp trusted-key number`  
To delete the key, use the `no ntp trusted-key number` command.

**Parameters** ***number*** Enter a number as the trusted key ID. The range is from 1 to 65534.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.14(0.0)</b>	The trusted-key range value is increased from 1 to 65534.
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The number parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.

**Related Commands** [ntp authentication-key](#) — sets an authentication key for NTP.  
[ntp authenticate](#) — enables the NTP authentication parameters you set.

# show clock

Displays 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

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Example**

```
Dell#show clock
12:30:04.402 pacific Tue May 22 2012
Dell#
```

**Example (Detail)**

```
Dell#show clock detail
12:30:26.892 pacific Tue May 22 2012
Time source is RTC hardware
Summer time starts 00:00:00 UTC Wed Mar 14 2012
Summer time ends 00:00:00 pacific Wed Nov 7 2012
Dell#
```



**Related Commands**

[clock summer-time recurring](#) — sets the software clock to convert to daylight saving time on a specific day each year.

## show ntp associations

Display the NTP master and peers.

**Syntax** `show ntp associations`

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ntp associations` command shown in the following example.

Field	Description
<b>(none)</b>	One or more of the following symbols could be displayed: <ul style="list-style-type: none"><li>* means synchronized to this peer.</li><li># means almost synchronized to this peer.</li><li>+ means the peer was selected for possible synchronization.</li><li>- means the peer is a candidate for selection.</li><li>x means designated falsesticker by the intersection algorithm.</li></ul>
<b>remote</b>	Displays the remote IP address of the NTP peer.
<b>ref clock</b>	Displays the IP address of the remote peer's reference clock.
<b>st</b>	Displays the peer's stratum, that is, the number of hops away from the external time source. A dash in this column means the NTP peer cannot reach the time source.
<b>when</b>	Displays the last time the switch received an NTP packet.
<b>poll</b>	Displays the polling interval (in seconds).
<b>reach</b>	Displays the reachability to the peer (in octal bitstream).
<b>delay</b>	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
<b>offset</b>	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
<b>disp</b>	Displays the dispersion.

**Example (without ntp master configuration)**

```
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#
```

**Example (with ntp master configuration)**

```
Dell EMC#show ntp associations
remote      vrf-Id    ref clock  st when poll reach  delay  offset  disp
=====
*LOCAL(0)   0         .LOCL.    7  6   16  377    0.000  0.000
0.002
```

```

10.16.127.86    0      10.16.127.26    5    9    16    1      65.292  13829.9
0.002
10.16.127.144  0      10.16.127.26    5    6    16    1      0.829   13795.2
0.002
10.16.127.44   0      10.16.127.26    5    -    16    1      0.799   13791.5
0.002
* master (synced), # backup, + selected, - outlier, x falseticker
Dell EMC#

```

**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

**Supported Modes** Full-Switch

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

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

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.6(0.0)</b>	Added support for VRF.
<b>9.4.(0.0)</b>	Added support for VRF.

## show ntp status

Display the current NTP status.

**Syntax** `show ntp status`

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show ntp status` command shown in the following example.

Field	Description
<b>“Clock is...”</b>	States whether the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
<b>“frequency is...”</b>	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
<b>“reference time is...”</b>	Displays the reference time stamp.

Field	Description
<b>“clock offset is...”</b>	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
<b>“root dispersion is...”</b>	Displays the root and path dispersion.
<b>“peer mode is...”</b>	State what NTP mode the switch is. This should be Client mode.

### Example

```
DellEMC# show ntp status
Clock is synchronized, stratum 4, reference is 10.16.151.117, vrf-id is 0
frequency is 0.000 ppm, stability is 0.000 ppm, precision is -18
reference time dec0e68a.07b308ac [Wed, Apr 7 0 9:42:34.030 UTC] UTC
clock offset is 0.000000 msec, root delay is 152.003 msec
root dispersion is 1381.293 msec, peer dispersion is 937.690 sec
peer mode is client
DellEMC#
```

### Related Commands

[show ntp associations](#) — displays information on the NTP master and peer configurations.

# Tunneling

Tunneling is supported on the Dell Networking OS.

## Topics:

- [tunnel-mode](#)
- [tunnel source](#)
- [tunnel keepalive](#)
- [tunnel allow-remote](#)
- [tunnel dscp](#)
- [tunnel destination](#)
- [tunnel flow-label](#)
- [tunnel hop-limit](#)
- [ip unnumbered](#)
- [ipv6 unnumbered](#)

## 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**

<b><i>ipip</i></b>	Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.
<b><i>ipv6</i></b>	Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.
<b><i>ipv6ip</i></b>	Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.
<b><i>decapsulate-any</i></b>	(Optional) Enable tunnel in multipoint receive-only mode.

**Defaults** None

**Command Modes** INTERFACE TUNNEL

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the decapsulate-any command.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** To enable a tunnel interface, use this command. You must define a tunnel mode for the tunnel to function. If you previously defined the tunnel destination or source address, the tunnel mode must be compatible.

Including the decapsulate-any option causes the command to fail if any of the following tunnel transmit options are configured: tunnel destination, tunnel dscp, tunnel flow-label, tunnel hop-limit, or tunnel keepalive. Conversely, if you configure any tunnel allow-remote entries, the `tunnel-mode` command fails unless the decapsulate-any option is included

Configuration of IPv6 commands over decapsulate-any tunnel causes an error.

# tunnel source

Set a source address for the tunnel.

<b>Syntax</b>	<code>tunnel source {ip-address   ipv6-address   interface-type-number}</code> To delete the current tunnel source address, use the <code>no tunnel source</code> command.						
<b>Parameters</b>	<p><b><i>ip-address</i></b> Enter the source IPv4 address in A.B.C.D format.</p> <p><b><i>ipv6-address</i></b> Enter the source IPv6 address in X:X:X:X::X format.</p> <p><b><i>interface-type-number</i></b></p> <ul style="list-style-type: none"><li>• For a Port Channel interface, enter the keywords <code>port-channel</code> then a number from 1 to 128.</li><li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li><li>• For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.</li></ul>						
<b>Defaults</b>	none						
<b>Command Modes</b>	INTERFACE TUNNEL (conf-if-tu)						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						
<b>Usage Information</b>	<p>If you configure a tunnel interface or destination address, the tunnel source must be compatible.</p> <p>If you configure a tunnel source address as an interface, the tunnel does not function until the compatible address is present on the particular interface.</p>						

# tunnel keepalive

Configure the tunnel keepalive target, interval and attempts.

<b>Syntax</b>	<code>tunnel keepalive {ip-address   ipv6-address}[interval {seconds}] [attempts {count   unlimited}]</code> Use the <b>no tunnel keepalive</b> command to disable tunnel keepalive probes.
<b>Parameters</b>	<p><b><i>ip-address ipv6 address</i></b> Enter the <b>IPv4 or IPv6 address</b> of the peer to which the keepalive probes will be sent.</p> <p><b><i>interval seconds</i></b> Enter the keyword <b>interval</b> followed by the interval time, in seconds, after which the restart process to keepalive probe packets. The range is from 5- 255. Default range is 5.</p> <p><b><i>count</i></b> (OPTIONAL) Enter the keyword <b>count</b> to count packets processed by the filter. The range is from 3-10, Default range is 3.</p> <p><b><i>unlimited</i></b> Enter the keyword <b>unlimited</b> to specify the unlimited number of keepalive probe packets.</p>
<b>Defaults</b>	Tunnel keepalive is disabled.
<b>Command Modes</b>	INTERFACE TUNNEL
<b>Supported Modes</b>	Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL.
<b>Usage Information</b>	When configured, the system will send ICMP echo probe packets at the configured interval and expect a response within the configured number of attempts, else the tunnel interface will be declared operational down.	

## tunnel allow-remote

Configure an IPv4 or IPv6 address or prefix whose tunneled packets will be accepted for decapsulation. If no allow-remote entries are configured, tunneled packets from any remote peer address will be accepted.

**Syntax** `tunnel allow-remote {ip-address | ipv6-address} [mask]`

Use the **no tunnel allow-remote** command to delete a configured allow-remote entry. Any specified address/mask values must match an existing entry for the delete to succeed. If the address and mask are not specified, this command deletes all allow-remote entries.

**Parameters**

**ip-address** Enter the source IPv4 address in A.B.C.D format.

**ipv6-address** Enter the source IPv6 address in X:X:X:X 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 no tunnel allow remote is configured, all traffic which is destined to tunnel source address will be decapsulated.

**Command Modes** INTERFACE TUNNEL

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL.

**Usage Information**

Up to eight allow-remote entries can be configured on any particular multipoint receive-only tunnel.

This command will fail 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 any allow-remote are configured, the tunnel source or tunnel mode commands will fail if the outer header address family does not match that of the configured allow-remote.

## tunnel dscp

Configure the method to set the DSCP in the outer tunnel header.

**Syntax** `tunnel dscp {mapped | <value>}`

To use the default tunnel mapping behavior, use the `no tunnel dscp value` command.

**Parameters**

**mapped** Enter the keyword `mapped` to map the original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

**value** Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of **0** denotes mapping of original packet DSCP (IPv4)/Traffic

Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

**Defaults** 0 (Mapped)

**Command Modes** INTERFACE TUNNEL (conf-if-tu)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 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**

<b><i>ip-address</i></b>	Enter the destination IPv4 address for the tunnel.
<b><i>ipv6-address</i></b>	Enter the destination IPv6 address for the tunnel.

**Defaults** none

**Command Modes** INTERFACE TUNNEL (conf-if-tu)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

**Syntax** `tunnel flow-label value`  
To return to the default value of 0, use the `no tunnel flow-label value` command.

**Parameters**

<b><i>value</i></b>	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 <b>0</b> .
---------------------	--

<b>Defaults</b>	0 (Mapped original packet flow-label value to tunnel header flow-label value)	
<b>Command Modes</b>	INTERFACE TUNNEL (conf-if-tu)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.

<b>Syntax</b>	<code>tunnel hop-limit value</code>	
	To restore the default tunnel hop-limit, use the <code>no tunnel hop-limit</code> command.	
<b>Parameters</b>	<b>value</b>	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 <b>64</b> .
<b>Defaults</b>	<b>64</b> (Time-to-live for IPv4 outer tunnel header or hop limit for IPv6 outer tunnel header)	
<b>Command Modes</b>	INTERFACE TUNNEL (conf-if-tu)	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.	

## ip unnumbered

Configure a tunnel interface to operate without a unique explicit IPv4 address and select the interface from which the tunnel will borrow its address.

<b>Syntax</b>	<b>ip unnumbered</b> <i>{interface-type interface-number}</i>	
	Use the <b>no ip unnumbered</b> command to set the tunnel back to default logical address. If the tunnel was previously operational, this will make the tunnel interface operationally down, unless the tunnel also has an IPv6 address configured..	
<b>Parameters</b>	<b>interface-type</b> <b>interface-number</b>	Enter the interface type, followed by a slot number.
<b>Defaults</b>	None	
<b>Command Modes</b>	INTERFACE TUNNEL	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.



**9.4(0.0)** Introduced on the MXL.

#### Usage Information

The ip unnumbered command will fail in two condition:

- If the logical ip address is configured.
- If the tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels the logical address route information should be present in both the ends.

**i** **NOTE:** The ip unnumbered command can specify an interface name that does not yet exist, or does not yet have a configured IPv6 address. The tunnel interface is not changed to the operationally up state until logically ip address is identified from the one of the address family.

## ipv6 unnumbered

Configure a tunnel interface to operate without a unique explicit IPv6 address and select the interface from which the tunnel will borrow its address.

**Syntax** **ipv6 unnumbered** *{interface-type interface-number}*

Use the **no ipv6 unnumbered** command to set the tunnel back to default logical address. If the tunnel was previously operational, this will make the tunnel interface operationally down, unless the tunnel also has an IPv4 address configured.

**Parameters** **interface-type** Enter the interface type, followed by the type, slot and port information.  
**interface-number**

**Defaults** None.

**Command Modes** INTERFACE TUNNEL

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Introduced on the MXL.

#### Usage Information

The ip unnumbered command will fail in two condition:

- If the logical ip address is configured.
- If the tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels the logical address route information should be present in both the ends.

**i** **NOTE:** The ipv6 unnumbered command can specify an interface name that does not yet exist, or does not yet have a configured IPv6 address. But the tunnel interface will not go operationally up until it has determined a logical address to use of at least one address family.

## u-Boot

All commands in this chapter are in u-Boot mode. These commands are supported on the Dell Networking Operating System (OS) FN IOM platform.

To access this mode, press any key when the following line appears on the console during a system boot.

```
Hit any key to stop autoboot:
```

Enter u-Boot immediately, as the `BOOT_USER#` prompt.

**NOTE:** This chapter describes only a few commands available in u-Boot mode.

**NOTE:** You cannot use the Tab key to complete commands in this mode.

### Topics:

- [boot change](#)
- [boot selection](#)
- [boot show net config retries](#)
- [boot write net config retries](#)
- [boot zero](#)
- [default gateway](#)
- [enable](#)
- [help](#)
- [ignore enable password](#)
- [ignore startup config](#)
- [interface management ethernet ip address](#)
- [no default-gateway](#)
- [no interface management ethernet ip address](#)
- [reload](#)
- [show boot blc](#)
- [show boot selection](#)
- [show bootflash](#)
- [show bootvar](#)
- [show default-gateway](#)
- [show interface management Ethernet](#)
- [show interface management port config](#)
- [syntax help](#)

## boot change

Change the operating system boot parameters.

**Syntax** `boot change [primary | secondary | default]`

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# boot selection

Change the ROM bootstrap bootflash partition.

**Syntax** boot selection [a | b]

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# boot show net config retries

Show the number of retries for network boot configuration failure.

**Syntax** boot show net config retries

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
BOOT_USER# boot show net config retries
Number of Network Boot Config Retries is : 0
BOOT_USER #
```

# boot write net config retries

Set the number of retries for network boot configuration failure.

**Syntax** boot write net config retries <int>

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
BOOT_USER # boot write net config retries 2
Updated number of Network Boot Config retries to 2.
BOOT_USER #
```

## boot zero

Clears the primary, secondary, or default boot parameters.

**Syntax** `boot zero [primary | secondary | default]`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## default gateway

Set the default gateway IP address.

**Syntax** `default-gateway <ip-address>`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## enable

Change the access privilege level.

**Syntax** `enable [user | admin]`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## help

Display the help menu.

**Syntax** `help`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]
    change operating system boot parameters
  boot selection [a|b]
    change the rom bootstrap bootflash partition
  boot show net config retries
    show number of retries for network boot config failure
  boot write net config retries <int>
    write number of retries for network boot config failure
  boot zero [primary|secondary|default]
    zero operating system boot parameters
  default-gateway <ip-address>
    default-gateway - set the default gateway ip address
  enable [user|admin]
    change access privilege level
  help
    display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #
```

## ignore enable password

Ignore the enabled password.

**Syntax** ignore enable-password

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## ignore startup config

Ignore the system startup configuration.

**Syntax** ignore startup-config

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## interface management ethernet ip address

Set the management port IP address and mask.

**Syntax** interface management ethernet ip address <ip/mask>

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## no default-gateway

Clear the default gateway IP address.

**Syntax** no default-gateway

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## no interface management ethernet ip address

Clear the management port IP address and mask.

**Syntax** no interface management ethernet ip address

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## reload

Reload the FN IOM switch.

**Syntax** reload

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# show boot blc

Show the boot loop counter value.

**Syntax** show boot blc

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # show boot blc ?
Total 1 possible command found.
Possible command list:
  show boot blc
  show the boot loop counter value
BOOT_USER # show boot blc
Boot_Loop Counter : 10

BOOT_USER #
```

# show boot selection

Display the ROM bootstrap bootflash partition.

**Syntax** show boot selection

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # show boot selection

ROM BOOTSTRAP SELECTOR PARMETERS:
=====
Next ROM bootstrap set to occur from Bootflash partition A.

Last ROM bootstrap occurred from Bootflash partition B.

BOOT_USER #
```

# show bootflash

Show summary of boot flash information.

**Syntax** show bootflash

**Command Modes** uBoot

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
=====
Bootflash Partition A:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Bootflash Partition B:
  Dell Force10 Networks System Boot
  Official IOM_LP_IMG_BOOT_LOADER, BSP Release 4.0.1.0bt1
  Created Tue May 1 10:56:16 2012 by build on login-sjc-01

Boot Selector Partition:
  Dell Force10 Networks System Boot
  Official IOM_XLOAD_LP_IMG_BOOT_SELECTOR, BSP Release 4.0.0.0bt1
  Created Tue May 1 10:56:34 2012 by build on login-sjc-01

BOOT_USER #
```

## show bootvar

Show summary of operating system boot parameters.

**Syntax** show bootvar

**Command Modes** uBoot

**Supported Modes** Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
=====
boot device                : tftp
file name                   : premnath
Management Ethernet IP address : 10.16.130.134/16
Server IP address          : 10.16.127.35
Default Gateway IP address  : 15.0.0.1
Management Ethernet MAC address : 00:01:E8:43:DE:DF

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
=====
No Operating System boot parameters specified!

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
=====
boot device                : tftp
file name                   : FTOS-XL-8-3-16-99.bin
Management Ethernet IP address : 10.16.130.134/16
Server IP address          : 10.16.127.53
Default Gateway IP address  : 15.0.0.1
Management Ethernet MAC address : 00:01:E8:43:DE:DF
```



```
BOOT_USER #
```

## show default-gateway

Display the default gateway IP address.

**Syntax** `show default-gateway`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # show default-gateway
Gateway IP address: 15.0.0.1
BOOT_USER #
```

## show interface management Ethernet

Show the management port IP address and mask.

**Syntax** `show interface management ethernet`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # show interface management ethernet
Management ethernet IP address: 10.16.130.134/16
BOOT_USER #
```

## show interface management port config

Show the management port boot characteristics.

**Syntax** `show interface management port config`

**Command Modes** uBoot

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # show interface management port config
Management ethernet Port Configuration: no Auto Negotiate
Management ethernet Port Configuration: 100M
Management ethernet Port Configuration: full duplex
BOOT_USER #
```

## syntax help

Show the syntax information.

**Syntax** help

**Command Modes** uBoot

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```
BOOT_USER # help
***** Dell Force10 Boot Interface Help Information *****
Current access level: USER LEVEL
Use "syntax help" for more information on syntax.
Available command list (22 commands total):
  boot change [primary|secondary|default]
    change operating system boot parameters
  boot selection [a|b]
    change the rom bootstrap bootflash partition
  boot show net config retries
    show number of retries for network boot config failure
  boot write net config retries <int>
    write number of retries for network boot config failure
  boot zero [primary|secondary|default]
    zero operating system boot parameters
  default-gateway <ip-address>
    default-gateway - set the default gateway ip address
  enable [user|admin]
    change access privilege level
  help
    display help menu
-(36%)-Use <CR> to continue, q to stop:
BOOT_USER #
```

# Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with network interface controller (NIC) teaming, automatic recovery from a failed link.

**NOTE:** In Standalone, VLT, and Stacking modes, the UFD group number is 1 by default and cannot be changed.

## Topics:

- [clear ufd-disable](#)
- [debug uplink-state-group](#)
- [defer-timer](#)
- [description](#)
- [downstream](#)
- [downstream auto-recover](#)
- [downstream disable links](#)
- [enable](#)
- [show running-config uplink-state-group](#)
- [show uplink-state-group](#)
- [uplink-state-group](#)
- [upstream](#)

## clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

**Syntax** `clear ufd-disable {interface interface | uplink-state-group group-id}`

### Parameters

<b>interface</b> <b><i>interface</i></b>	Specify one or more downstream interfaces. For <i>interface</i> , enter one of the following interface types: <ul style="list-style-type: none"> <li>• 10 Gigabit Ethernet: <code>tengigabitethernet {slot/port   slot/ port-range}</code></li> <li>• Port channel: <code>port-channel {1-512   port-channel-range}</code></li> </ul> Where <code>port-range</code> and <code>port-channel-range</code> specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: <code>tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5</code> . A comma is required to separate each port and port-range entry.
<b>uplink-state-group</b> <b><i>group-id</i></b>	Re-enables all UFD-disabled downstream interfaces in the group. The valid <i>group-id</i> values are from 1 to 16.

**Defaults** A downstream interface in a UFD-disabled uplink-state group is also disabled and is in a UFD-Disabled Error state.

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)

Full-Switch

### Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

Version	Description
9.2(0.0)	Supported on the M I/O Aggregator.

**Related Commands**

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

## debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

**Syntax** `debug uplink-state-group [group-id]`  
 To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

**Parameters** **group-id** Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
 Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

**Related Commands** [clear ufd-disable](#) — re-enables downstream interfaces that are in a UFD-Disabled Error state.

## defer-timer

Configure a timer that prevents unwanted flapping of downstream ports when the uplink port channel goes down and comes up.

**Syntax** `defer-timerseconds`

**Defaults** 10 (Standalone mode)

**Parameters** **seconds** Specify the time (in seconds) to wait for the upstream port channel (LAG 128) to come back up before server ports are brought down. The range is from 1 to 120.

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Standalone, Stacking, VLT  
 Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

## Usage Information

This command is not supported in Programmable-Mux mode.

# description

Enter a text description of an uplink-state group.

**Syntax** `description text`

**Parameters** **text** Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.

**Defaults** none

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

## Example

```
Dell(conf-uplink-state-group-16)# description test
Dell(conf-uplink-state-group-16)#
```

## Related Commands

[uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

# downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

**Syntax** `downstream interface`

To delete an uplink-state group, enter the `no downstream interface` command.

**Parameters** **interface** Enter one of the following interface types:

- 10 Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

**Defaults** none

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

## Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.

Version	Description
9.4(0.0)	Supported on the FN I/O Aggregator.

#### Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

#### Related Commands

- [upstream](#) — assigns a port or port-channel to the uplink-state group as an upstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

## downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

**Syntax** `downstream auto-recover`

To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.

**Defaults** The auto-recovery of UFD-disabled downstream ports is enabled.

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

#### Related Commands

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

## downstream disable links

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

**Syntax** `downstream disable links {number | all}`

To revert to the default setting, use the `no downstream disable links` command.

#### Parameters

<b><i>number</i></b>	Enter the number of downstream links to be brought down by UFD. The range is from 1 to 1024.
<b><i>all</i></b>	Brings down all downstream links in the group.

**Defaults** No downstream links are disabled when an upstream link in an uplink-state group goes down.

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Supported on the M I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.
<b>Version</b>	<b>Description</b>								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.								
<b>Usage Information</b>	<p>A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down.</p> <p>If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.</p>								
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>• <a href="#">downstream</a> — assigns a port or port-channel to the uplink-state group as a downstream interface.</li> <li>• <a href="#">uplink-state-group</a> — creates an uplink-state group and enables the tracking of upstream links.</li> </ul>								

## enable

Re-enable upstream-link tracking for an uplink-state group after it has been disabled.

<b>Syntax</b>	<p><code>enable</code></p> <p>To disable upstream-link tracking without deleting the uplink-state group, use the <code>no enable</code> command.</p>
<b>group-id</b>	Enables debugging on the specified uplink-state group. Valid <i>group-id</i> values are 1 to 16.
<b>Defaults</b>	Upstream-link tracking is automatically enabled in an uplink-state group.
<b>Command Modes</b>	UPLINK-STATE-GROUP
<b>Supported Modes</b>	All Modes

<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> <tr> <td><b>9.2(0.0)</b></td> <td>Supported on the M I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.
<b>Version</b>	<b>Description</b>								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.								

## show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

<b>Syntax</b>	<code>show running-config uplink-state-group [<i>group-id</i>]</code>						
<b>Parameters</b>	<p><b><i>group-id</i></b> Displays the current configuration of all uplink-state groups or a specified group. The valid <i>group-id</i> values are from 1 to 16.</p>						
<b>Defaults</b>	none						
<b>Command Modes</b>	<ul style="list-style-type: none"> <li>• EXEC</li> <li>• EXEC Privilege</li> </ul>						
<b>Supported Modes</b>	<p>Programmable-Mux (PMUX)</p> <p>Full-Switch</p>						
<b>Command History</b>	<table border="0"> <thead> <tr> <th style="text-align: left;"><b>Version</b></th> <th style="text-align: left;"><b>Description</b></th> </tr> </thead> <tbody> <tr> <td><b>9.9(0.0)</b></td> <td>Introduced on the FN IOM.</td> </tr> <tr> <td><b>9.4(0.0)</b></td> <td>Supported on the FN I/O Aggregator.</td> </tr> </tbody> </table>	<b>Version</b>	<b>Description</b>	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>Version</b>	<b>Description</b>						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.						

Version	Description
9.2(0.0)	Supported on the M I/O Aggregator.

### Example

```
Dell#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream TengigabitEthernet 0/2,4,6,11
upstream TengigabitEthernet 0/8, 12
upstream PortChannel 1
!
uplink state track 2
downstream TengigabitEthernet 0/1,3,5
upstream TengigabitEthernet 0/9,10
```

### Related Commands

- [show uplink-state-group](#) — displays the status information on a specified uplink-state group or all groups.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

## show uplink-state-group

Display status information on a specified uplink-state group or all groups.

**Syntax** `show uplink-state-group [group-id] [detail]`

**Parameters**

<b>group-id</b>	Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
<b>detail</b>	Displays additional status information on the upstream and downstream interfaces in each group

**Defaults** none

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

### Example

```
Dell#show uplink-state-group detail

(Up): Interface up      (Dwn): Interface down   (Dis): Interface disabled

Uplink State Group      : 1          Status: Enabled, Up
Defer Timer              : 10 sec
Upstream Interfaces     : Po 128(Up)
Downstream Interfaces   : Te 0/1(Dwn) Te 0/2(Dwn) Te 0/3(Up) Te 0/4(Dwn)
Te 0/5(Up)
                        Te 0/6(Dwn) Te 0/7(Up) Te 0/8(Up)

Dell#
```



**Related Commands**

- [show running-config uplink-state-group](#) — displays the current configuration of one or more uplink-state groups.
- [uplink-state-group](#) — create an uplink-state group and enables the tracking of upstream links.

## uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

**Syntax** `uplink-state-group group-id`  
To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

**Parameters** **group-id** Enter the ID number of an uplink-state group. The range is from 1 to 16.

**Defaults** none

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information**

After you enter the command, to assign upstream and downstream interfaces to the group, enter Uplink-State-Group Configuration mode.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in uplink-state-group configuration mode.

**Example**

```
Dell(conf)#uplink-state-group 16
Dell(conf)#
02:23:17: %RPM0-P:CP %IFMGR-5-ASTATE_UP: Changed uplink state group
Admin state to up: Group 16
```

**Related Commands**

- [show running-config uplink-state-group](#) — displays the current configuration of one or more uplink-state groups.
- [show uplink-state-group](#) — displays the status information on a specified uplink-state group or all groups.

## upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

**Syntax** `upstream interface`  
To delete an uplink-state group, use the `no upstream interface` command.

**Parameters** **interface** Enter one of the following interface types:

- 10 Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 0/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

**Defaults** none

**Command Modes** UPLINK-STATE-GROUP

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

**Usage Information**

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

**Example**

```
Dell(conf-uplink-state-group-16)# upstream tengigabitethernet 0/1-5
Dell(conf-uplink-state-group-16)#
```

**Related Commands**

- [downstream](#) — assigns a port or port-channel to the uplink-state group as a downstream interface.
- [uplink-state-group](#) — creates an uplink-state group and enables the tracking of upstream links.

# VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can “stack” VLANs into one tunnel and switch them through the network transparently.

For more information about basic VLAN commands, 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.
- 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 OS 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.

### Topics:

- [dei enable](#)
- [dei honor](#)
- [dei mark](#)
- [member](#)
- [show interface dei-honor](#)
- [show interface dei-mark](#)
- [vlan-stack access](#)
- [vlan-stack compatible](#)
- [vlan-stack dot1p-mapping](#)
- [vlan-stack protocol-type](#)
- [vlan-stack trunk](#)

## dei enable

Make packets eligible for dropping based on their drop eligible indicator (DEI) value.

<b>Syntax</b>	<code>dei enable</code>	
<b>Defaults</b>	Packets are colored green; no packets are dropped.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

# dei honor

Honor the incoming DEI value by mapping it to a system drop precedence. Enter the command once for 0 and once for 1.

<b>Syntax</b>	<code>dei honor {0   1} {green   red   yellow}</code>	
<b>Parameters</b>	<b>0   1</b>	Enter the bit value you want to map to a color.
	<b>green   red   yellow</b>	Choose a color: <ul style="list-style-type: none"><li>• Green: High priority packets that are the least preferred to be dropped.</li><li>• Yellow: Lower priority packets that are treated as best-effort.</li><li>• Red: Lowest priority packets that are always dropped (regardless of congestion status).</li></ul>
<b>Defaults</b>	Disabled; Packets with an unmapped DEI value are colored green.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	You must first enable DEI for this configuration to take effect.	
<b>Related Commands</b>	<a href="#">dei enable</a> — enables DEI.	

# dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

<b>Syntax</b>	<code>dei mark {green   yellow} {0   1}</code>	
<b>Parameters</b>	<b>0   1</b>	Enter the bit value you want to map to a color.
	<b>green   yellow</b>	Choose a color: <ul style="list-style-type: none"><li>• Green: High priority packets that are the least preferred to be dropped.</li><li>• Yellow: Lower priority packets that are treated as best-effort.</li></ul>
<b>Defaults</b>	All the packets on egress are marked with DEI 0.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	You must first enable DEI for this configuration to take effect.	
<b>Related Commands</b>	<a href="#">dei enable</a> — enables DEI.	

# 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 information.

**Defaults** Not configured.

**Command Modes** `conf-if-vl-<vlan-id>-stack`

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

# show interface dei-honor

Display the dei honor configuration.

**Syntax** `show interface dei-honor [interface slot/port]`

**Parameters** ***interface slot/port*** Enter the interface type then the line card slot and port number.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Example

```
Dell#show interface dei-honor

Default Drop precedence: Green
Interface   CFI/DEI      Drop precedence
-----
Te 0/1     0             Green
Te 0/1     1             Yellow
Te 1/9     1             Red
Te 1/12    0             Yellow
```

```
Dell#show interface dei-honor
```

```

Default Drop precedence: Green
Interface    CFI/DEI      Drop precedence
-----
Te 0/1      0             Green
Te 0/1      1             Yellow
Te 1/2      1             Red
Te 1/3      0             Yellow

```

**Related Commands** [dei honor](#) — honors the incoming DEI value.

## show interface dei-mark

Display the dei mark configuration.

**Syntax** `show interface dei-mark [interface slot/port]`

**Parameters** *interface slot/port* Enter the interface type then the line card slot and port number.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

### Example

```

Dell#show interface dei-mark

Default CFI/DEI Marking: 0
Interface    Drop precedence    CFI/DEI
-----
Te 0/1      Green              0
Te 0/1      Yellow             1
Te 8/9      Yellow             0
Te 8/12     Yellow             0

```

**Related Commands** [dei mark](#) — sets the DEI value on egress.

## 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

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## 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

## Supported Modes

Full-Switch

## Command History

Version	Description
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## Usage Information

Prior to disabling the stackable VLAN feature, remove the members.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

## Example

```
Dell#show vlan
Codes: * - Default VLAN, G - GVRP VLANs

  NUM  Status   Q Ports
*  1    Inactive
  2    Active   M Te 1/2
                        M Te 1/0-2
  3    Active   M Po1(Te 1/3-4)
                        M Te 1/5
                        M Te 1/3
  4    Active   M Po1(Te 1/3-5)
                        M Te 1/6
                        M Te 1/4
  5    Active   M Po1(Te 1/5-6)
                        M Te 1/6
                        M Te 1/5
Dell#
```

# vlan-stack dot1p-mapping

Map C-Tag dot1p values to an 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 if there is conflicts.

## Syntax

`vlan-stack dot1p-mapping c-tag-dot1p values sp-tag-dot1p value`

## Parameters

<b>c-tag-dot1p value</b>	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 5.
<b>sp-tag-dot1p value</b>	Enter the keyword <code>sp-tag-dot1p</code> then the service provider dot1p value. The range is from 0 to 5.

## Defaults

none

**Command Modes** INTERFACE

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## vlan-stack protocol-type

Define the stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, the system assigns the value 0x9100.

**Syntax** `vlan-stack protocol-type number`

**Parameters** *number* Enter the hexadecimal number as the stackable VLAN tag.  
You may specify both bytes of the 2-byte S-Tag TPID. The range is from 0 to FFFF. The default is **9100**.

**Defaults** 0x9100

**Command Modes** CONFIGURATION

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** For specific interoperability limitations regarding the S-Tag TPID, refer to the *Dell Networking OS Configuration Guide*.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 the 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 the first example, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In the second example, the tag protocol identifier (TPID) is set to 8848. The “Gi 3/10” Te 3/8 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 the [Interfaces](#) chapter.

### Example

```
Dell(conf-if-Te-0/12)#switchport
Dell(conf-if-Te-0/12)#vlan-stack trunk
Dell(conf-if-Te-0/12)#show config
!
interface TenGigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
Dell(conf-if-Te-0/42)#interface vlan 100
Dell(conf-if-vl-100)#vlan-stack compatible
Dell(conf-if-vl-100-stack)#member TenGigabitEthernet 0/12
Dell(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member TenGigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-100-stack)#interface vlan 20
Dell(conf-if-vl-20)#tagged TengigabitEthernet 0/12
Dell(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged TenGigabitEthernet 0/12
  shutdown
Dell(conf-if-vl-20)#do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

  NUM  Status Description      Q Ports
*  1    Inactive
  20   Active                T Te 0/12
  100  Active                M Te 0/12
Dell(conf-if-vl-20)#
```

### Example

```
Dell(config)#vlan-stack protocol-type 88A8
Dell(config)#interface TenGigabitEthernet 3/8
Dell(conf-if-te-3/8)#no shutdown
Dell(conf-if-te-3/8)#switchport
Dell(conf-if-te-3/8)#vlan-stack access
Dell(conf-if-te-3/8)#exit

Dell(config)#interface TenGigabitEthernet 8/0
Dell(conf-if-te-10/0)#no shutdown
Dell(conf-if-te-10/0)#portmode hybrid
Dell(conf-if-te-10/0)#switchport
Dell(conf-if-te-10/0)#vlan-stack trunk
Dell(conf-if-te-10/0)#exit
```

```
Dell(config)#interface vlan 20
Dell(conf-if-vlan)#vlan-stack compatible
Dell(conf-if-vlan)#member Te 7/0, te 3/8, TenGi 8/0
Dell(conf-if-vlan)#exit
```

```
Dell(config)#interface vlan 20
Dell(conf-if-vlan)#untagged TenGi 8/0
Dell(conf-if-vlan)#exit
Dell(config)#
```

```
Dell(config)#interface vlan 40
Dell(conf-if-vlan)#tagged TenGi 8/0
Dell(conf-if-vlan)#exit
Dell(config)#
```

## Virtual Link Trunking (VLT)

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.

**i 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.

### Topics:

- [back-up destination](#)
- [clear ip mroute](#)
- [clear ip pim tib](#)
- [clear vlt statistics](#)
- [delay-restore abort-threshold](#)
- [lACP ungroup member-independent](#)
- [multicast peer-routing timeout](#)
- [peer-link port-channel](#)
- [peer-routing](#)
- [peer-routing-timeout](#)
- [primary-priority](#)
- [show ip mroute](#)
- [show vlt backup-link](#)
- [show vlt brief](#)
- [show vlt detail](#)
- [show vlt inconsistency](#)
- [show vlt mismatch](#)
- [show vlt role](#)
- [show vlt statistics](#)
- [stack-unit iom-mode](#)
- [system-mac](#)
- [unit-id](#)
- [vlt domain](#)
- [vlt-peer-lag port-channel](#)
- [show vlt private-vlan](#)

## 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.

<b>Syntax</b>	<code>back-up destination {[ipv4-address]   [ipv6 ipv6-address] [interval seconds]}</code>	
<b>Parameters</b>	<b>ipv4-address</b>	Enter the IPv4 address of the backup destination.
	<b>ipv6</b>	Enter the keyword <code>ipv6</code> then an IPv6 address in the X:X:X::X format.
	<b>interval seconds</b>	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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

## 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.

<b>Syntax</b>	<code>clear ip mroute {group-address [source-address]   *   snooping}</code>	
<b>Parameters</b>	<b>group-address [source-address]</b>	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
	<b>*</b>	Enter * to clear all multicast routes.
	<b>snooping</b>	Enter the keyword <code>snooping</code> to delete multicast snooping route table entries.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## clear ip pim tib

Clear PIM tree information from the PIM database.

<b>Syntax</b>	<code>clear ip pim tib [group]</code>	
<b>Parameters</b>	<b>group</b>	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 entries in Peer PIM TIB (Sync) are not deleted but are marked for re-download. Both local and synced routes are removed from the 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.

## clear vlt statistics

Clear the statistics on VLT operations.

**Syntax** `clear vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]`

<b>Parameters</b>		
<b>domain</b>		Clear the VLT statistics for the domain.
<b>multicast</b>		Clear the VLT statistics for multicast.
<b>mac</b>		Clear the VLT statistics for the MAC address.
<b>arp</b>		Clear the VLT statistics for ARP.
<b>igmp-snoop</b>		Clear the VLT statistics for IGMP snooping.
<b>ndp</b>		Clear the VLT statistics for NDP.

**Command Modes** EXEC

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

### 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
```

## delay-restore abort-threshold

Increase the Boot Up timer to some value (>60 seconds).

**Syntax** `delay-restore abort-threshold <interval>`

To remove use the `no delay-restore abort-threshold` command.

**Defaults** 60 seconds

**Command Modes** VLT DOMAIN

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.7(0.0)	Introduced on Supported on the MXL 10/40GbE Switch IO Module.

**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**

<b>port-channel</b>	Force all LACP port-channel members to become switchports.
<b>vlt</b>	Force all VLT LACP members to become switchports.

**Defaults** Not configured.

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

**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.

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.

<b>Syntax</b>	<code>multicast peer-routing timeout value</code> To restore the default value, use the <code>no multicast peer-routing timeout</code> command.						
<b>Parameters</b>	<b>value</b> Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.						
<b>Default</b>	Not configured.						
<b>Command Modes</b>	VLT DOMAIN (conf-vlt-domain)						
<b>Supported Modes</b>	Full-Switch						
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Introduced on the MXL 10/40GbE Switch IO Module.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
Version	Description						
<b>9.9(0.0)</b>	Introduced on the FN IOM.						
<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.						

# peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

<b>Syntax</b>	<code>peer-link port-channel port-channel-number {peer-down-vlan vlan id}</code>								
<b>Parameters</b>	<b>port-channel-number</b> Enter the port-channel number that acts as the interconnect trunk. <b>peer-down-vlan vlan id</b> 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.								
<b>Defaults</b>	Not configured.								
<b>Command Modes</b>	VLT DOMAIN								
<b>Supported Modes</b>	Programmable-Mux (PMUX) Full-Switch								
<b>Command History</b>	<table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td><b>9.9(0.0)</b></td><td>Introduced on the FN IOM.</td></tr><tr><td><b>9.4(0.0)</b></td><td>Supported on the FN I/O Aggregator.</td></tr><tr><td><b>9.2(0.0)</b></td><td>Supported on the M I/O Aggregator.</td></tr></tbody></table>	Version	Description	<b>9.9(0.0)</b>	Introduced on the FN IOM.	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.
Version	Description								
<b>9.9(0.0)</b>	Introduced on the FN IOM.								
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.								
<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.								
<b>Usage Information</b>	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 <b>peer-down-vlan</b> parameter. 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.

<b>Syntax</b>	<code>peer-routing</code> To disable L3 VLT peer-routing, use the <code>no peer-routing</code> command.
<b>Defaults</b>	Disabled.

**Command Modes** VLT DOMAIN (conf-vlt-domain)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the IPV6/IPV4 support on the MXL.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## peer-routing-timeout

Configure the timeout for the software to wait before connecting to a VLT peer with a Down status. This command is applicable for both IPV6/ IPV4.

**Syntax** `peer-routing-timeout value`  
To restore the default value, use the `no peer-routing-timeout` command.

**Parameters** **value** Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).

**Command Modes** VLT DOMAIN (conf-vlt-domain)

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Added the IPV6/IPV4 support on the MXL.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

Reconfigure the primary role of VLT peer switches.

**Syntax** `primary-priority value`

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** After you configure the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the software elects a primary and secondary VLT peer device. To reconfigure the primary role of VLT peer switches, use the `priority` command.



# show ip mroute

View the multicast routing table.

<b>Syntax</b>	<code>show ip mroute [static   group-address [source-address]   count   snooping [vlan vlan-id] [group-address [source-address]]   summary   vlt [group-address   count]</code>	
<b>Parameters</b>	<b>Static</b>	(OPTIONAL) Enter the keyword <code>static</code> to view static multicast routes.
	<b>group-address [source-address]</b>	(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.
	<b>count</b>	(OPTIONAL) Enter the keyword <code>count</code> to view the number of multicast routes and packets.
	<b>snooping [vlan vlan-id] [group-address [source-address]]</b>	(OPTIONAL) Enter the keyword <code>snooping</code> 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.
	<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to view routes in a tabular format.
	<b>vlt</b>	(OPTIONAL) Enter the keyword <code>vlt</code> 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.
	<b>count</b>	Enter the keyword <code>count</code> to display VLT route and packet data.
<b>Command Modes</b>	<ul style="list-style-type: none"><li>EXEC</li><li>EXEC Privilege</li></ul>	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.2(0.0)</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	The following describes the <code>show ip mroute</code> command shown in the examples.	
	<b>Field</b>	<b>Description</b>
	<b>(S, G)</b>	Displays the forwarding entry in the multicast route table.
	<b>uptime</b>	Displays the amount of time the entry has been in the multicast forwarding table.
	<b>Incoming interface</b>	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
<b>Outgoing interface list:</b>	Lists the interfaces that meet one of the following: <ul style="list-style-type: none"><li>a directly connected member of the Group</li><li>statically configured member of the Group</li><li>received a (*,G) or (S,G) Join message</li></ul>	

### 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 4/1

(*, 225.1.2.1), uptime 00:04:16
Incoming vlan: Vlan 2
Outgoing interface list:
TenGigabitEthernet 4/2
TenGigabitEthernet 4/3

(165.87.1.7, 225.1.2.1), uptime 00:03:17
Incoming vlan: Vlan 2
Outgoing interface list:
TenGigabitEthernet 4/1
TenGigabitEthernet 4/2
TenGigabitEthernet 4/3
TenGigabitEthernet 4/4
TenGigabitEthernet 4/5
```

### Example (detail)

```
Dell#show ip mroute
IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
Incoming interface: TenGigabitEthernet 3/1
Outgoing interface list:
GigabitEthernet 3/2

(1.13.1.100, 224.10.10.1), uptime 00:04:03
Incoming interface: TenGigabitEthernet 3/4
Outgoing interface list:
TenGigabitEthernet 3/4
TenGigabitEthernet 3/5

(*, 224.20.20.1), uptime 00:05:12
Incoming interface: TenGigabitEthernet 3/2
Outgoing interface list:
TenGigabitEthernet 3/4
Outgoing interface 1
TenGigabitEthernet 3/3
```

## show vlt backup-link

Displays information on the backup link operation.

**Syntax** show vlt backup-link

**Default** Not configured.

**Command Modes** EXEC

**Supported Modes** All Modes

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.4(0.0)**

Supported on the FN I/O Aggregator.

Version	Description
9.2(0.0)	Supported on the M I/O Aggregator.

#### Example

```
Dell# show vlt backup-link
VLT Backup Link
-----
Destination:                169.254.31.23
Peer HeartBeat status:      Up
HeartBeat Timer Interval:   1
HeartBeat Timeout:          3
UDP Port:                   34998
HeartBeat Messages Sent:    24
HeartBeat Messages Received: 25
```

## show vlt brief

Display brief status information about VLT domains currently configured on the switch.

<b>Syntax</b>	show vlt brief
<b>Default</b>	Not configured.
<b>Command Modes</b>	EXEC
<b>Supported Modes</b>	All Modes

#### Command History

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

#### 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 detail

Displays detailed status information about VLT domains currently configured on the switch.

<b>Syntax</b>	show vlt detail
<b>Default</b>	Not configured.

**Command Modes** EXEC

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

**Example**

```
Dell# show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
-----
128          128          UP          UP          1000
Dell#
```

## show vlt inconsistency

Display deviations in VLT multicast traffic.

**Syntax** show vlt inconsistency ip mroute

**Command Modes** EXEC

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell#show vlt inconsistency ip mroute
Spanned Multicast Routing IIF Inconsistency

Multicast Route          LocalIIF          PeerIIF
-----
(22.22.22.200, 225.1.1.2)  VLAN 5           VLAN 6
(*, 225.1.1.2)           VLAN 15          te 0/5
Dell#
```

## show vlt mismatch

Display mismatches in VLT parameters.

**Syntax** show vlt mismatch

**Command Modes** EXEC

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.
9.2(0.0)	Supported on the M I/O Aggregator.

## Example

```
Dell#show vlt mismatch
Domain
-----
Parameters          Local          Peer
-----
Unit-ID             0              15

Vlan-config
-----
Vlan-ID             Local Mode     Peer Mode
-----
100                  --            L3

Vlan IPV4 Multicast Status
-----
Vlan-ID             Local Status   Peer Status
-----
4094                 Active         Inactive

Dell#
```

## show vlt role

Display 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 locally-attached VLT device.

**Syntax** show vlt role

**Default** Not configured.

**Command Modes** EXEC

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

## Example

```
Dell#show vlt role
VLT Role
-----
VLT Role:                Primary
System MAC address:      00:01:05:08:02:05
Primary Role Priority:    32768
Local System MAC address: 00:01:e8:00:ab:03
Local System Role Priority: 32768
Local Unit Id:           0

Dell#
```

## show vlt statistics

Displays statistics on VLT operations.

**Syntax** show vlt statistics

**Default** Not configured.

**Command Modes** EXEC

**Supported Modes** All Modes

**Command History**

<b>Version</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**Example**

```
Dell#show vlt statistics
VLT Domain Statistics
-----
HeartBeat Messages Sent:      449
HeartBeat Messages Received:  448
ICL Hello's Sent:             154
ICL Hello's Received:         154
Domain Mismatch Errors:       0
Version Mismatch Errors:      0
Config Mismatch Errors:       0

VLT MAC Statistics
-----
L2 Info Pkts sent:16, L2 Mac-sync Pkts Sent:25
L2 Info Pkts Rcvd:15, L2 Mac-sync Pkts Rcvd:24
L2 Reg Request sent:2
L2 Reg Request rcvd:1
L2 Reg Response sent:1
L2 Reg Response rcvd:1

VLT Igmp-Snooping Statistics
-----
IGMP Info Pkts sent:      9
IGMP Info Pkts Rcvd:     10
IGMP Reg Request sent:    2
IGMP Reg Request rcvd:   2
IGMP Reg Response sent:  2
IGMP Reg Response rcvd:  1
IGMP PDU Tunnel Pkt sent: 0
IGMP PDU Tunnel Pkt rcvd: 0
IGMP Tunnel PDUs sent:   0
IGMP Tunnel PDUs rcvd:   0

VLT ARP Statistics
-----
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP Tunnel Pkts sent Non Vlt:0
ARP Tunnel Pkts Rcvd Non Vlt:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:2
ARP Reg Request rcvd:1
VLT IOA Statistics
-----
IOA Info Pkts sent:      5
IOA Info Pkts Rcvd:      7
IOA Reg Request sent:    2
IOA Reg Request rcvd:    2
IOA Reg Response sent:   2
IOA Reg Response rcvd:   1
VLT NDP Statistics
-----
NDP NA VLT Tunnel Pkts sent:0
NDP NA VLT Tunnel Pkts Rcvd:0
NDP NA Non-VLT Tunnel Pkts sent:0
NDP NA Non-VLT Tunnel Pkts Rcvd:0
Ndp-sync Pkts Sent:0
Ndp-sync Pkts Rcvd:0
Ndp Reg Request sent:2
```

```
Ndp Reg Request rcvd:1
VLT multicast not enabled
```

## stack-unit iom-mode

Set the switch operating mode to VLT mode.

**Syntax** `stack-unit <unit-number> iom-mode vlt`

**Parameters**

<b>unit number</b> <0-5>	Enter the number of the member stack unit. The range is from 0 to 5. The default is 0.
<b>vlt</b>	Enable virtual link trunking mode.

**Command Modes** CONFIGURATION

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** This command resets the operating mode to VLT. You must reboot the switch after using this command.

## system-mac

Reconfigure the default MAC address for the domain.

**Syntax** `system-mac mac-address`

**Parameters**

<b>mac-address</b>	Enter the system MAC address for the VLT domain.
--------------------	--

**Defaults** Not configured.

**Command Modes** VLT DOMAIN

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** When you create a VLT domain on a switch, Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations.

To reconfigure the default MAC address for the domain by entering a new MAC address in the format nn:nn:nn:nn:nn:nn, use the `system-mac` command.

You must also reconfigure the same MAC address on the VLT peer switch.

# unit-id

Explicitly configure the default unit ID of a VLT peer switch.

**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

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**Usage Information** When you create a VLT domain on a switch, Dell Networking OS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. Configure a different unit ID (0 or 1) on each peer switch.

To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.

# vlt domain

Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

**Syntax** `vlt domain domain-id`

**Parameters** **domain-id** Enter the Domain ID number. Configure the same domain ID on the peer switch. The range of domain IDs is from 1 to 1000.

**Command Modes** CONFIGURATION

**Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>9.2(0.0)</b>	Supported on the M I/O Aggregator.

**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.



# 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** *id-number* Enter the respective vlt port-channel number of the peer device.
- Defaults** Not configured.
- Command Modes** INTERFACE PORT-CHANNEL
- Supported Modes** Programmable-Mux (PMUX)  
Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.
	9.2(0.0)	Supported on the M I/O Aggregator.

# show vlt private-vlan

Display the association of private VLAN (PVLAN) with the VLT LAG. You can configure VLT peer nodes in a PVLAN on the switch.

- Syntax** `show vlt private-vlan`
- Command Modes** EXEC
- Supported Modes** Full-Switch

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.3(0.0)	Introduced on the MXL 10/40GbE Switch IO Module platform.

**Usage Information** If you add an ICL or VLTi link as a member of a primary VLAN, the ICL becomes a part of the primary VLAN and its associated secondary VLANs, similar to the behavior for normal trunk ports. VLAN symmetry is not validated if you associate an ICL to a PVLAN. Similarly, if you dissociate an ICL from a PVLAN, although the PVLAN symmetry exists, ICL is removed from that PVLAN in such a case. The **ICL Status** field denotes the type of the VLAN port of the VLTi link configured in a PVLAN.

### Example

```
Dell#Show vlt private-vlan vlan-id

Codes: C- Community, I - Isolated, V - Internally tagged, T - tagged, *
- VLT Pvlan
Primary      Secondary      ICL Status
10           20 (C)         V
              30 (I)         V

40           50 (C)         T
              60 (I)         T

Dell#
```

# Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking Operating System (OS) for IPv4 and IPv6.

The following commands apply to both VRRP IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- track
- virtual-address

VRRP Ipv6 are in the [VRRP for IPv6 Commands](#) section.

## Topics:

- [advertise-interval](#)
- [authentication-type](#)
- [clear counters vrrp](#)
- [debug vrrp](#)
- [description](#)
- [disable](#)
- [hold-time](#)
- [preempt](#)
- [priority](#)
- [show config](#)
- [show vrrp](#)
- [track](#)
- [virtual-address](#)
- [vrrp delay minimum](#)
- [vrrp delay reload](#)
- [vrrp-group](#)
- [VRRP for IPv6 Commands](#)
- [clear counters vrrp ipv6](#)
- [debug vrrp ipv6](#)
- [show vrrp ipv6](#)
- [vrrp-ipv6-group](#)
- [version](#)

## advertise-interval

Set the time interval between VRRP advertisements.

**Syntax**                    `advertise-interval {seconds | centisecs centisecs}`

To return to the default settings, use the `no advertise-interval` command.

**Parameters**                **seconds**                    Enter a number of seconds. The range is from 1 to 255. The default is **1 second**.

**centisecs**                      Enter the keyword `centisecs` followed by the number of centisecs in multiple of  
**centisecs**                      25 centisecs. The range is 25 to 4075 centisecs in multiples of 25 centisecs.

**Defaults**                      **1 second or 100 centisecs**

**Command Modes**            INTERFACE-VRRP

**Supported Modes**           Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the support for centisecs on the MXL 10/40GbE Switch .
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**            Dell Networking OS 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**

<b>simple</b>	Enter the keyword <code>simple</code> to specify simple authentication.
<b>encryption-type</b>	(OPTIONAL) Enter one of the following numbers: <ul style="list-style-type: none"><li>• 0 (zero) specifies an un-encrypted authentication data follows.</li><li>• 7 (seven) specifies a hidden authentication data follows.</li></ul>
<b>password</b>	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

**Supported Modes**           Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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]`


**Parameters**                      **vrrp-id**                      (OPTIONAL) Enter the number of the VRRP group ID. The range is from 1 to 255.

**Command Modes**            EXEC Privilege

**Supported Modes**           Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

 **NOTE:** This command also enables you to clear the port configurations corresponding to a range of ports.

- You can specify multiple ports as slot/port-range. For example, if you want to clear the port configurations corresponding to all ports between 1 and 4, specify the port range as `clear counters interfaces interface-type 1/1 - 4`.

## debug vrrp

Allows you to enable debugging of VRRP.

<b>Syntax</b>	<code>debug vrrp interface [vrrp-id] {all   packets   state   timer}</code>	
	To disable debugging, use the <code>no debug vrrp interface [vrrp-id] {all   packets   state   timer}</code> command.	
<b>Parameters</b>	<b>interface</b>	Enter the following keywords and slot/port or number information <ul style="list-style-type: none"> <li>For Port Channel interface types, enter the keywords <code>port-channel</code> then the number. The range is from 1 to 128.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.</li> </ul>
	<b>vrrp-id</b>	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
	<b>all</b>	Enter the keyword <code>all</code> to enable debugging of all VRRP groups.
	<b>packets</b>	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
	<b>state</b>	Enter the keyword <code>state</code> to enable debugging of VRRP state changes.
	<b>timer</b>	Enter the keyword <code>timer</code> to enable debugging of the VRRP timer.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** If you do not specify options, debug is active on all interfaces and all VRRP groups.

## description

Configure a short text string describing the VRRP group.

<b>Syntax</b>	<code>description text</code>	
	To delete a VRRP group description, use the <code>no description</code> command.	
<b>Parameters</b>	<b>text</b>	Enter a text string up to 80 characters long.

<b>Defaults</b>	Not enabled.	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## disable

Disable a VRRP group.

<b>Syntax</b>	<code>disable</code>	
	To re-enable a disabled VRRP group, use the <code>no disable</code> command.	
<b>Defaults</b>	Enabled.	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	To enable VRRP traffic, assign an IP address to the VRRP group using the <code>virtual-address</code> command and enter <code>no disable</code> .	
<b>Related Commands</b>	<a href="#">virtual-address</a> — 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.

<b>Syntax</b>	<code>hold-time {seconds   centiseconds centiseconds}</code>	
	To return to the default value, use the <code>no hold-time</code> command.	
<b>Parameters</b>	<b>seconds</b>	Enter a number of seconds. The range is from 0 to 65535. The default is <b>zero (0) seconds</b> .
	<b>centiseconds centiseconds</b>	Enter the keyword <code>centiseconds</code> then the number of centiseconds in units of 25 centiseconds. The range is from 0 to 65525 in units of 25 centiseconds.
<b>Defaults</b>	<b>zero (0) seconds</b>	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.5(0.0)</b>	Introduced the support for centiseconds on the MXL 10/40GbE Switch.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	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.
<b>Related Commands</b>	<a href="#">disable</a> — disables a VRRP group.

## preempt

To preempt or become the MASTER router, permit a BACKUP router with a higher priority value.


<b>Syntax</b>	<code>preempt</code>	To prohibit preemption, use the <code>no preempt</code> command.
<b>Defaults</b>	Enabled (that is, a BACKUP router can preempt the MASTER router).	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## priority

Specify a VRRP priority value for the VRRP group. The VRRP protocol uses this value during the MASTER election process.

<b>Syntax</b>	<code>priority <i>priority</i></code>	To return to the default value, use the <code>no priority</code> command.
<b>Parameters</b>	<b><i>priority</i></b>	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 <b>100</b> .
<b>Defaults</b>	<b>100</b>	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

<b>Usage Information</b>	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 <code>priority</code> command to 255 and the <code>virtual-address</code> is not equal to the interface's primary IP address, an error message appears.
--------------------------	---

 **NOTE:** Configuring VRRP priority 255 on an interface on which DHCP Client is enabled is not supported.

# show config

View the non-default VRRP configuration.

**Syntax** `show config [verbose]`

**Parameters** **verbose** (OPTIONAL) Enter the keyword `verbose` to view all VRRP group configuration information, including defaults.

**Command Modes** VRRP

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Example**

```
Dell(conf-if-vrid-4)#show con
vrrp-group 4
virtual-address 119.192.182.124
!
```

# show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the system returns `No Active VRRP group.`

**Syntax** `show vrrp [vrrp-id] [interface] [brief]`

**Parameters**

- vrrp-id** (OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. The range is from 1 to 255.
- interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For Port Channel interface types, enter the keywords `port-channel` then the number. The range is from 1 to 128.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 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.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show vrrp brief` command shown in the following example.

Item	Description
<b>Interface</b>	Lists the interface type, slot and port on which the VRRP group is configured.
<b>Grp</b>	Displays the VRRP group ID.

Item	Description
<b>Pri</b>	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.
<b>Pre</b>	States whether preempt is enabled on the interface. <ul style="list-style-type: none"> <li>• Y = Preempt is enabled.</li> <li>• N = Preempt is not enabled.</li> </ul>
<b>State</b>	Displays the operational state of the interface by using one of the following: <ul style="list-style-type: none"> <li>• NA/IF (the interface is not available).</li> <li>• MASTER (the interface associated with the MASTER router).</li> <li>• BACKUP (the interface associated with the BACKUP router).</li> </ul>
<b>Master addr</b>	Displays the IP address of the MASTER router.
<b>Virtual addr(s)</b>	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-----
TenGig 1/9 1 100 Y Master 200.200.200.200 200.200.200.201
TenGig 1/9 2 100 Y Master 200.200.200.200 200.200.200.202
200.200.200.203
Description
TenGig1/9 3 100 Y Master 1.1.1.1 1.1.1.2
TenGig1/9 4 100 Y Master 200.200.200.200 200.200.200.206
200.200.200.207 ... short
desc

Dell>
```

### Usage Information

The following describes the `show vrrp` command shown in the following example.

Item	Description
<b>State: master...</b>	Displays the interface's state: <ul style="list-style-type: none"> <li>• Na/If (not available)</li> <li>• master (MASTER virtual router)</li> <li>• backup (BACKUP virtual router)</li> </ul> the interface's priority and the IP address of the MASTER.
<b>Hold Down:...</b>	This line displays additional VRRP configuration information: <ul style="list-style-type: none"> <li>• Hold Down displays the hold down timer interval in seconds.</li> <li>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</li> <li>• AdvInt displays the Advertise Interval in seconds.</li> </ul>
<b>Adv rcvd:...</b>	This line displays counters for the following: <ul style="list-style-type: none"> <li>• Adv rcvd displays the number of VRRP advertisements received on the interface.</li> <li>• Adv sent displays the number of VRRP advertisements sent on the interface.</li> <li>• Gratuitous ARP sent displays the number of gratuitous ARPs sent.</li> </ul>
<b>Virtual MAC address</b>	Displays the virtual MAC address of the VRRP group.
<b>Virtual IP address</b>	Displays the virtual IP address of the VRRP router to which the interface is connected.
<b>Authentication:...</b>	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
<b>Tracking states..</b>	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:



Item	Description
	<ul style="list-style-type: none"> <li>• Dn or Up states whether the interface is down or up.</li> <li>• the interface type slot/port information.</li> </ul>

### Example

```
Dell>show vrrp
-----
TenGigabitEthernet 1/3, VRID: 1, Net: 10.1.1.253
VRF: 0 default
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 1/13 priority-cost 10
-----
TenGigabitEthernet 1/4, VRID: 2, Net: 10.1.2.253
VRF: 0 default
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
    00:00:5e:00:01:02
Virtual IP address:
    10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
    Up TenGigabitEthernet 2/1 priority-cost 10
    Up TenGigabitEthernet 3/8 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 or number information:
		<ul style="list-style-type: none"> <li>• For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.</li> <li>• For Port Channel interface types, enter the keywords <code>port-channel</code> then the number. The range is from 1 to 128.</li> <li>• For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>• For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.</li> </ul>
	<i>cost</i>	(OPTIONAL) Enter a number as the amount to be subtracted from the priority value. The range is 1 to 254. The default is <b>10</b> .

**Defaults** `cost = 10`

**Command Modes** VRRP

**Supported Modes** Full-Switch

Command History	Version	Description

<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

<b>Syntax</b>	<code>virtual-address ip-address1 [... ip-address12]</code>	
	To delete one or more virtual IP addresses, use the <code>no virtual-address ip-address1 [... ip-address12]</code> command.	
<b>Parameters</b>	<b><i>ip-address1</i></b>	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.
	<b><i>... ip-address12</i></b>	(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.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	VRRP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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 <code>virtual-address</code> 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.

<b>Syntax</b>	<code>vrrp delay minimum seconds</code>	
<b>Parameters</b>	<b><i>seconds</i></b>	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).
<b>Defaults</b>	0	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.

**8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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

**Supported Modes** Full-Switch


<b>Command History</b>	<b>Version</b>	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	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.	
<b>Related Command</b>	<a href="#">virtual-address</a> — assigns up to 12 virtual IP addresses per VRRP group.	

## VRRP for IPv6 Commands

The following commands apply to IPv6.

### clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

<b>Syntax</b>	<code>clear counters vrrp ipv6 [vrid   vrf instance]</code>	
<b>Parameters</b>	<b>vrid</b>	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is from 1 to 255.
	<b>vrf instance</b>	(OPTIONAL) Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.
<b>Defaults</b>	Not configured	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.
<b>Usage Information</b>	 <b>NOTE:</b> This command also enables you to clear the port configurations corresponding to a range of ports.	
	<ul style="list-style-type: none"> <li>You can specify multiple ports as slot/port-range. For example, if you want to clear the port configurations corresponding to all ports between 1 and 4, specify the port range as <code>clear counters interfacesinterface-type 1/1 - 4</code>.</li> </ul>	

### debug vrrp ipv6

Allows you to enable debugging of VRRP.

<b>Syntax</b>	<code>debug vrrp ipv6 interface [vrid] {all   packets   state   timer}</code>	
<b>Parameters</b>	<b>interface</b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.</li> </ul>
	<b>vrid</b>	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.

<b>all</b>	Enter the keyword <code>all</code> to enable debugging of all VRRP groups.
<b>packets</b>	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
<b>state</b>	Enter the keyword <code>state</code> to enable debugging of VRRP state changes
<b>timer</b>	Enter the keyword <code>timer</code> to enable debugging of the VRRP timer.

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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 system returns `No Active VRRP group.`

**Syntax** `show vrrp ipv6 [vrid] [interface] [brief]`

<b>Parameters</b>	<b>vrid</b>	(OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.
	<b>interface</b>	Enter the following keywords and slot/port or number information: <ul style="list-style-type: none"> <li>For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.</li> <li>For SONET interfaces, enter the keyword <code>sonet</code> then the slot/port information.</li> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> <li>For a VLAN interface, enter the keyword <code>vlan</code> then the VLAN ID. The VLAN ID range is from 1 to 4094.</li> </ul>
	<b>brief</b>	(OPTIONAL) Enter the keyword <code>brief</code> to view a table of information on the VRRP groups.

**Command Modes**

- EXEC
- EXEC Privilege

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information** The following describes the `show vrrp ipv6` command shown in the following example.

Line Beginning with	Description
<b>GigabitEthernet..</b> .	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.
<b>State: master...</b>	Displays the interface's state: <ul style="list-style-type: none"> <li>Na/If (not available).</li> <li>master (MASTER virtual router).</li> </ul>

Line	Description
<b>Beginning with</b>	<ul style="list-style-type: none"> <li>• backup (BACKUP virtual router).</li> </ul> <p>the interface's priority and the IP address of the MASTER.</p>
<b>Hold Down:...</b>	<p>This line displays additional VRRP configuration information:</p> <ul style="list-style-type: none"> <li>• Hold Down displays the hold down timer interval in seconds.</li> <li>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</li> <li>• AdvInt displays the Advertise Interval in seconds.</li> </ul>
<b>Adv rcvd:...</b>	<p>This line displays counters for the following:</p> <ul style="list-style-type: none"> <li>• Adv rcvd displays the number of VRRP advertisements received on the interface.</li> <li>• Adv sent displays the number of VRRP advertisements sent on the interface.</li> <li>• Bad pkts rcvd displays the number of invalid packets received on the interface.</li> </ul>
<b>Virtual MAC address</b>	Displays the virtual MAC address of the VRRP group.
<b>Virtual IP address</b>	Displays the virtual IP address of the VRRP router to which the interface is connected.
<b>Tracking states...</b>	<p>Displays information on the tracked interfaces or objects configured for a VRRP group (<code>track</code> command), including:</p> <ul style="list-style-type: none"> <li>• UP or DOWN state of the tracked interface or object (Up or Dn).</li> <li>• Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object.</li> <li>• Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.</li> </ul>

### Example

```
Dell#show vrrp ipv6
-----
GigabitEthernet 5/6, IPv6 VRID: 255, Version: 3, Net:
fe80::201:e8ff:fe7a:6bb9
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.

<b>Syntax</b>	<code>vrrp-ipv6-group vrid</code>	
<b>Parameters</b>	<b><i>vrid</i></b>	Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	INTERFACE	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	Description

- 9.9(0.0)** Introduced on the FN IOM.
- 8.3.16.1** Introduced on the MXL 10/40GbE Switch IO Module.

**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 OS or non-Dell Networking OS) in the same VRRP group in order for all routers to interoperate.

## version

Set the VRRP protocol version for the IPv4 group.

**Syntax** `version {2 | 3 | both}`

To return to the default setting, use the `no version` command.

<b>Parameters</b>	<b>2</b>	Enter the keyword <code>2</code> to specify VRRP version 2 as defined by RFC 3768, <i>Virtual Router Redundancy Protocol</i> .
	<b>3</b>	Enter the keyword <code>3</code> to specify VRRP version 3 as defined by RFC 5798, <i>Virtual Router Redundancy Protocol</i> .
	<b>both</b>	Enter the keyword <code>both</code> for in-service migration from VRRP version 2 to VRRP version 3.

**Defaults** 2

**Command Modes** VRRP

**Supported Modes** Full-Switch

**Command History** This guide is platform-specific. For command information about other platforms, see 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</b>	<b>Description</b>
<b>9.9(0.0)</b>	Introduced on the FN IOM.
<b>9.7(0.0)</b>	Introduced on the S6000-ON..
<b>9.5(0.0)</b>	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

**Usage Information**

You can use the `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 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-vrid-100)#version ?
2      VRRPv2
3      VRRPv3
both   Interoperable, send VRRPv3 receive both

Dell(conf-if-te-1/1-vrid-100)#version 3
```



## SNMP Traps

This chapter lists the traps sent by the Dell Networking Operating System (OS). Each trap is listed by the fields Message ID, Trap Type, and Trap Option.

**Table 6. SNMP Traps and Error Messages**

Message ID	Trap Type	Trap Option
<b>COLD_START</b>	SNMP	COLDSTART
%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.		
<b>WARM_START</b>	SNMP	WARMSTART
<b>COPY_CONFIG_COMPLETE</b>	SNMP	NONE
SNMP Copy Config Command Completed		
<b>LINK_DOWN</b>	SNMP	LINKDOWN
%IFA-1-PORT_LINKDN: changed interface state to down:%d		
<b>LINK_UP</b>	SNMP	LINKUP
%IFA-1-PORT_LINKUP: changed interface state to up:%d		
<b>AUTHENTICATION_FAIL</b>	SNMP	AUTH
%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.		
<b>EGP_NEIGHBOR_LOSS</b>	SNMP	NONE
<b>OSTATE_DOWN</b>	SNMP	LINKDOWN
%IFM-1-OSTATE_DN: changed interface state to down:%s %IFM-5-CSTATE_DN:Changed interface Physical state to down: %s		
<b>OSTATE_UP</b>	SNMP	LINKUP
%IFM-1-OSTATE_UP: changed interface state to up:%s %IFM-5-CSTATE_UP: Changed interface Physical state to up: %s		
<b>RMON_RISING_THRESHOLD</b>	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>		
<b>RMON_FALLING_THRESHOLD</b>	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>		
<b>RMON_HC_RISHING_THRESHOLD</b>	SNMP	NONE
%RPM0-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>		
<b>RMON_HC_FALLING_THRESHOLD</b>	SNMP	NONE

**Table 6. SNMP Traps and Error Messages (continued)**

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>		
<b>RESV</b>	NONE	NONE
<b>N/A</b>		
<b>CHM_MIN_ALARM_TEMP</b>	ENVMON	TEMP
%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature		
<b>CHM_MIN_ALARM_TEMP_CLR</b>	ENVMON	TEMP
%CHMRG-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)		
<b>CHM_MAJ_ALARM_TEMP</b>	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)		
<b>CHM_MAJ_ALARM_TEMP_CLR</b>	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)		
<b>TME_TASK_SUSPEND</b>	ENVMON	NONE
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
<b>TME_TASK_TERM</b>	ENVMON	NONE
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
<b>CHM_CPU_THRESHOLD</b>	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
<b>CHM_CPU_THRESHOLD_CLR</b>	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
<b>CHM_MEM_THRESHOLD</b>	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
<b>CHM_MEM_THRESHOLD_CLR</b>	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
<b>MACMGR_STN_MOVE</b>	ENVMON	NONE
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
<b>VRRP_BDAUTH</b>	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		
<b>VRRP_GO_MASTER</b>	PROTO	NONE

**Table 6. SNMP Traps and Error Messages (continued)**

Message ID	Trap Type	Trap Option
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		
<b>VRRP_PROTOCOL_ERROR</b>	PROTO	NONE
VRRP_PROTOERR: VRRP protocol error on %S		
<b>BGP4_ESTABLISHED</b>	PROTO	NONE
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
<b>BGP4_BACKW_XSITION</b>	PROTO	NONE
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		
<b>ETS_TRAP_TYPE_MODULE_STATUS_CHANGE</b>	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to enabled %DIFFSERV-5-ETS_TRAP_TYPE_MODULE_STATUS_CHANGE: ETS Module status changed to disabled		
<b>ETS_TRAP_TYPE_ADMIN_MODE_CHANGE</b>	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to on for port %s %DIFFSERV-5-ETS_TRAP_TYPE_ADMIN_MODE_CHANGE : ETS Admin mode changed to off for port %s		
<b>ETS_TRAP_TYPE_OPER_STATE_CHANGE</b>	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to init for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to off for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to recommended for port %s %DIFFSERV-5-ETS_TRAP_TYPE_OPER_STATE_CHANGE: ETS Oper state changed to rxConfigSrc for port %s		
<b>ETS_TRAP_TYPE_PEER_STATE_CHANGE</b>	ETS	NONE
%DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to enabled for port %s %DIFFSERV-5-ETS_TRAP_TYPE_PEER_STATE_CHANGE : ETS Peer state changed to disabled for port %s		
<b>PFC_TRAP_TYPE_MODULE_STATUS_CHANGE</b>	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to enabled %DIFFSERV-5-PFC_TRAP_TYPE_MODULE_STATUS_CHANGE: PFC Module status changed to disabled		
<b>PFC_TRAP_TYPE_ADMIN_MODE_CHANGE</b>	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to on for port %s %DIFFSERV-5-PFC_TRAP_TYPE_ADMIN_MODE_CHANGE : PFC Admin mode changed to off for port %s		
<b>PFC_TRAP_TYPE_OPER_STATE_CHANGE</b>	PFC	NONE

**Table 6. SNMP Traps and Error Messages (continued)**

Message ID	Trap Type	Trap Option
%DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to init for port %s %DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to off for port %s %DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to recommended for port %s %DIFFSERV-5-PFC_TRAP_TYPE_OPER_STATE_CHANGE: PFC Oper state changed to rxConfigSrc for port %s		
<b>PFC_TRAP_TYPE_PEER_STATE_CHANGE</b>	PFC	NONE
%DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to enabled for port %s %DIFFSERV-5-PFC_TRAP_TYPE_PEER_STATE_CHANGE: PFC Peer state changed to disabled for port %s		
<b>FIPS_MAX_FCF_LIMIT_RCH</b>	FIPS	NONE
%FCOE-5-MAX_FCF_LIMIT_RCH: Number of FCFs reached maximum allowed limit in VLAN %d		
<b>FIPS_MAX_ENODE_LIMIT_RCH</b>	FIPS	NONE
%FCOE-5-MAX_ENODE_LIMIT_RCH: Number of ENodes reached maximum allowed limit in the system		
<b>FIPS_MAX_SESSION_LIMIT_RCH</b>	FIPS	NONE
%FCOE-5-MAX_SESSION_LIMIT_RCH: Number of sessions reached maximum allowed limit in the system		
<b>FIPS_FCF_DROP</b>	FIPS	NONE
%FCOE-5-FCF_DROP: New FCF(%d,%s) discovered in Vlan %d is dropped as max-FCF-limit per VLAN is reached		
<b>FIPS_ENODE_DROP</b>	FIPS	NONE
%FCOE-5-ENODE_DROP: New ENode(%d,%s) discovered in interface %s dropped as max-ENode-limit in system reached		
<b>FIPS_SESSION_DROP</b>	FIPS	NONE
%FCOE-5-SESSION_DROP: New session(%d,%s) request in interface %s dropped as max-session-limit in system reached		
<b>FIPS_ACL_INSTALL_FAIL</b>	FIPS	NONE
%FCOE-5-ACL_INSTALL_FAIL: problem in installing ACL entries due to no space or hardware failure		
<b>CHMGR_ENT_LAST_CHANGE_TIME</b>	ENTITY	NONE
No error messages. Time, at which there is a change in a physical entity, is logged.		

## FC Flex IO Modules

This part provides a generic, broad-level description of the operations, capabilities, and configuration commands of the Fiber Channel (FC) Flex IO module.

FC Flex IO Module mentioned in this guide refers to FCF Port Combo Card.

### Topics:

- [FC Flex IO Modules](#)
- [Data Center Bridging \(DCB\) for FC Flex IO Modules](#)
- [NPIV Proxy Gateway for FC Flex IO Modules](#)

## FC Flex IO Modules

This part provides a generic, broad-level description of the operations, capabilities, and configuration commands of the Fiber Channel (FC) Flex IO module.

## Data Center Bridging (DCB) for FC Flex IO Modules

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

The Fibre Channel (FC) Flex IO module is supported on switch. The switch installed with the FC Flex IO module functions as a top-of-rack edge switch that supports converged enhanced ethernet (CEE) traffic — Fibre Channel over Ethernet (FCoE) for storage, inter-process communication (IPC) for servers, and Ethernet local area network (LAN) (IP cloud) for data — and FC links to one or more storage area network (SAN) fabrics.

The `dcb-input` and `dcb-output` configuration commands are deprecated, starting with Dell Networking OS Release 9.3(0.0) on the Dell switches. Use the `dcp-map` command to create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic.

The Dell Networking Operating System (OS) commands for the DCB features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

## NPIV Proxy Gateway for FC Flex IO Modules

The N-port identifier virtualization (NPIV) Proxy Gateway (NPG) feature provides FCoE-FC bridging capability on the system with the FC Flex IO module switch, allowing server CNAs to communicate with SAN fabrics over the FN IOM with the FC Flex IO module.

To configure the FN IOM with the FC Flex IO module to operate as an NPIV proxy gateway, use the following commands:

### description (for FCoE maps)

In an FCoE map, add a text description of the FCoE and FC parameters used to transmit storage traffic over a Switch with the FC Flex IO module NPIV proxy gateway in a converged fabric.

<b>Syntax</b>	<code>description text</code>	
<b>Parameters</b>	<b><i>text</i></b>	Enter a maximum of 32 characters.
<b>Defaults</b>	None	

**Command Modes** FCOE MAP

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.3(0.0)**

Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

The text description is displayed in `show fcoe-map` command output.

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fabric

Apply an FCoE map on a fabric-facing Fibre Channel (FC) port.

**Syntax** `fabric map-name`

**Parameters** **map-name** Maximum: 32 alphanumeric characters.

**Defaults** None

**Command Modes** INTERFACE FIBRE\_CHANNEL

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.3(0.0)**

Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on a switch with the FC Flex IO module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric. Use the `fcoe-map` command to create an FCoE map.

On a switch with the FC Flex IO module NPIV proxy gateway, you cannot apply an FCoE map on fabric-facing FC ports and server-facing Ethernet ports.

After you apply an FCoE map on an FC interface, when the port is enabled (`no shutdown`), the NPIV proxy gateway starts sending FIP multicast advertisements on behalf of the FC port to downstream servers in order to advertise the availability of a new FCF port on the FCoE VLAN.

To remove an FCoE map from an FC interface, enter the `no fabric map-name` command in Interface configuration mode.

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fabric-id vlan

In an FCoE map, configure the association between the dedicated VLAN used to carry FCoE traffic between servers and a SAN, and the fabric where the desired storage arrays are installed.

**Syntax** `fabric-id fabric-num vlan vlan-id`

**Parameters**

<b>fabric-id fabric-num</b>	Enter a fabric ID number that is the same as the ID number of the dedicated VLAN used to carry FCoE storage traffic to the fabric specified in the FCoE map. You can enter a fabric ID in the range 1–4094.
<b>vlan vlan-id</b>	Enter the ID number of the dedicated VLAN used to carry FCoE storage traffic between servers and a SAN fabric and specified with the <code>vlan</code> command in the FCoE map.

**Defaults** None

**Command Modes** FCOE MAP

**Supported Modes** Full–Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

In the `fabric-id vlan` command, the fabric and VLAN ID numbers must be the same.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique.

To remove a fabric-VLAN association from an FCoE map, enter the `no fabric-id vlan` command.

You must first create a VLAN and then specify the configured VLAN ID in the `fabric-id vlan` command. Otherwise, the following error message is displayed.

```
FTOS(conf-fcoe-f)#fabric-id 10 vlan 10 % Error: Vlan 10 does not exist
```

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fcf-priority

In an FCoE map, configure the priority used by a server CNA to select an upstream FCoE forwarder (FCF).

**Syntax** `fcf-priority priority`

**Parameters**

<b>priority</b>	Enter the priority assigned to the switch with the FC Flex IO module NPIV proxy gateway, which appears to a downstream server CNA as an FCF. The range of FCF priority values is from 1 to 255.
-----------------	---

**Defaults** 128

**Command Modes** FCOE MAP

**Supported Modes** Full–Switch

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

<b>Usage Information</b>	<p>The FCF priority you assign to the Switch with the FC Flex IO module is used by server CNAs to select an upstream FCF to use for a fabric login (FLOGI).</p> <p>To remove a configured FCF priority from an FCoE map, enter the <code>no fcf-priority</code> command.</p>
<b>Related Commands</b>	<p><a href="#">fcoe-map</a> — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.</p> <p><a href="#">show fcoe-map</a> — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.</p>

## fc-map

In an FCoE map, configure the FCoE mapped address prefix (FC-MAP) value which is used to identify FCoE traffic transmitted on the FCoE VLAN for the specified fabric.

<b>Syntax</b>	<code>fc-map fc-map-value</code>	
<b>Parameters</b>	<b><i>fc-map-value</i></b>	Enter the unique MAC address prefix used by a SAN fabric. The range of FC-MAP values is from 0EFC00 to 0EFCFF.
<b>Defaults</b>	None	
<b>Command Modes</b>	FCoE MAP	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.6(0.0)</b>	Supported on the FN 2210S Aggregator.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

<b>Usage Information</b>	<p>The FC-MAP value you enter must match the FC-MAP value used by an FC switch or FCoE forwarder (FCF) in the fabric. An FCF switch accepts only FCoE traffic that uses the correct FC-MAP value.</p> <p>The FC-MAP value is used to generate the fabric-provided MAC address (FP-MAC). The FPMA is used by servers to transmit FCoE traffic to the fabric. An FC-MAP can be associated with only one FCoE VLAN and vice versa.</p> <p>In an FCoE map, the FC-MAP value, fabric ID, and FCoE VLAN parameters must be unique.</p> <p>To remove a configured FC-MAP value from an FCoE map, enter the <code>no fc-map</code> command.</p>
--------------------------	---

<b>Related Commands</b>	<p><a href="#">fcoe-map</a> — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.</p> <p><a href="#">show fcoe-map</a> — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.</p>
-------------------------	---

## fcoe-map

Create an FCoE map which contains the parameters used to configure the links between server CNAs and a SAN fabric. Apply the FCoE map on a server-facing Ethernet port.

<b>Syntax</b>	<code>fcoe-map map-name</code>	
<b>Parameters</b>	<b><i>map-name</i></b>	Maximum: 32 alphanumeric characters.
<b>Defaults</b>	None	
	On the I/O Aggregator with FC Flex IO modules, the following parameters are applied on all the FC Flex IO module interfaces:	



- Description: SAN\_FABRIC
- Fabric-id: 1002
- Fcoe-vlan: 1002
- Fc-map: 0x0efc00
- Fcf-priority: 128
- Fka-adv-period: 8000mSec
- Keepalive: enable
- Vlan priority: 3

**Command Modes** CONFIGURATION  
INTERFACE

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

### Usage Information

An FCoE map is a template used to map FCoE and FC parameters in a converged fabric. An FCoE map is used to virtualize upstream FC ports on the switch with the FC Flex IO module NPIV proxy gateway so that they appear to downstream server CNA ports as FCoE forwarder (FCF) ports on an FCoE network. When applied to FC and Ethernet ports on an NPIV proxy gateway, an FCoE map allows the switch to operate as an FCoE-FC bridge between an FC SAN and an FCoE network by providing FCoE-enabled servers and switches with the necessary parameters to log in to a SAN fabric.

On a switch with the FC Flex IO module NPIV proxy gateway, you cannot apply an FCoE map is applied on fabric-facing FC ports and server-facing 10-Gigabit Ethernet ports.

An FCoE map consists of the following parameters: the dedicated FCoE VLAN used for storage traffic, the destination SAN fabric (FC-MAP value), FCF priority used by a server, and the FIP keepalive (FKA) advertisement timeout.

In each FCoE map, the fabric ID, FC-MAP value, and FCoE VLAN parameters must be unique. Use one FCoE map to access one SAN fabric. You cannot use the same FCoE map to access different fabrics.

To remove an FCoE map from an Ethernet interface, enter the `no fcoe-map map-name` command in Interface configuration mode.

### Related Commands

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## fka-adv-period

In an FCoE map, configure the time interval used to transmit FIP keepalive (FKA) advertisements.

**Syntax** `fka-adv-period seconds`

**Parameters** **seconds** Enter the time period (in seconds) used to send FIP keepalive messages to peer devices. The range is from 8 to 90 seconds.

**Defaults** 8 seconds

**Command Modes** FCOE MAP

**Supported Modes** Full-Switch

<b>Command History</b>	<b>Version</b>	<b>Version</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3(0.0)</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.
<b>Usage Information</b>	To delete the FIP keepalive time period from an FCoE map, enter the <code>no fka-adv-erpiod</code> command.	
<b>Related Commands</b>	<p><code>fcoe-map</code> — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.</p> <p><code>show fcoe-map</code> — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.</p>	

## interface vlan (NPIV proxy gateway)

Create a dedicated VLAN to be used to send and receive Fibre Channel traffic over FCoE links between servers and a fabric over a switch with the FC Flex IO module NPIV proxy gateway.

<b>Syntax</b>	<code>interface vlan <i>vlan-id</i></code>	
<b>Parameters</b>	<b><i>vlan-id</i></b>	Enter a number as the VLAN Identifier. The range is 1 to 4094.
<b>Defaults</b>	Not configured.	
<b>Command Modes</b>	CONFIGURATION	
<b>Supported Modes</b>	Full-Switch	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.3.0.0</b>	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module configured as an NPIV proxy gateway.
<b>Usage Information</b>	<p>FCoE storage traffic received from servers on a switch with the FC Flex IO module NPIV proxy gateway is de-capsulated into Fibre Channel packets and forwarded over FC links to SAN switches in a specified fabric. You must configure a separate FCoE VLAN for each fabric to which FCoE traffic is forwarded. Any non-FCoE traffic sent on a dedicated FCoE VLAN will be dropped.</p> <p>You configure the association between a dedicated VLAN, which carries FCoE traffic from server CNAs over the NPIV proxy gateway to a SAN fabric in which destination storage arrays are installed, in an FCoE map by using the <code>fabric id vlan</code> command.</p> <p>When you apply an FCoE map to a server-facing Ethernet port, the port is automatically configured as a tagged member of the FCoE VLAN.</p> <p>For more information about VLANs and the commands to configure them, refer to the <a href="#">Virtual LAN (VLAN) Commands</a> section of the <a href="#">Layer 2</a> chapter.</p>	
<b>Example (Single Range)</b>	<pre>FTOS(conf)#interface vlan 10 FTOS(conf-if-vl-3)#</pre>	
<b>Related Commands</b>	<p><code>fcoe-map</code> — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.</p> <p><code>show fcoe-map</code>— displays the Fibre Channel and FCoE configuration parameters in FCoE maps.</p>	

## keepalive

In an FCoE map, enable the monitoring of FIP keepalive messages (if it is disabled).

**Syntax** `keepalive`

**Parameters** None

**Defaults** FIP keepalive monitoring is enabled on Ethernet and Fibre Channel interfaces.

**Command Modes** FCOE MAP

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.3(0.0)**

Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

FIP keepalive (FKA) messaging is used to detect if other FCoE devices are reachable.

To remove FIP keepalive monitoring from an FCoE map, enter the `no keepalive` command.

**Related Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

[show fcoe-map](#) — displays the Fibre Channel and FCoE configuration parameters in FCoE maps.

## show fcoe-map

Display the Fibre Channel and FCoE configuration parameters in FCoE maps.

**Syntax** `show fcoe-map [brief | map-name]`

**Parameters**

**brief**

Displays an overview of currently configured FCoE maps.

**map-name**

Displays the FC and FCoE configuration parameters in a specified FCoE map. The FCoE map is applied on Ethernet (FCoE) and FC ports to transmit FC storage traffic to a specified fabric.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

**Version**

**Description**

**9.9(0.0)**

Introduced on the FN IOM.

**9.3(0.0)**

Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

Use the `show fcoe-map` command to display the FC and FCoE parameters used to configure server-facing Ethernet (FCoE) and fabric-facing FC ports in all FCoE maps on a switch with the FC Flex IO module NPIV proxy gateway.

In each FCoE map, the values for the fabric ID and FC-MAP that identify the SAN fabric to which FC storage traffic is sent, and the FCoE VLAN to be used must be unique.

An FCoE map is used to identify the SAN fabric to which FCoE storage traffic is sent and to virtualize the switch with the FC Flex IO module FC ports so that they appear to downstream server CNA ports as FCoE Forwarder (FCF) ports on an FCoE network.

The following table describes the `show fcoe-map brief` output shown in the example below.

Field	Description
<b>Fabric-Name</b>	Name of a SAN fabric.
<b>Fabric ID</b>	The ID number of the SAN fabric to which FC traffic is forwarded.
<b>VLAN ID</b>	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
<b>FC-MAP</b>	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
<b>FCF Priority</b>	The priority used by a server to select an upstream FCoE forwarder.
<b>Config-State</b>	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
<b>Oper-State</b>	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).

The following table describes the `show fcoe-map map-name` output shown in the example below.

Field	Description
<b>Fabric-Name</b>	Name of a SAN fabric.
<b>Fabric ID</b>	The ID number of the SAN fabric to which FC traffic is forwarded.
<b>VLAN ID</b>	The dedicated FCoE VLAN used to transport FCoE storage traffic between servers and a fabric over the NPIV proxy gateway. The configured VLAN ID must be the same as the fabric ID.
<b>VLAN priority</b>	FCoE traffic uses VLAN priority 3. (This setting is not user-configurable.)
<b>FC-MAP</b>	FCoE MAC address-prefix value - The unique 24-bit MAC address prefix that identifies a fabric.
<b>FKA-ADV-period</b>	Time interval (in seconds) used to transmit FIP keepalive advertisements.
<b>FCF Priority</b>	The priority used by a server to select an upstream FCoE forwarder.
<b>Config-State</b>	Indicates whether the configured FCoE and FC parameters in the FCoE map are valid: Active (all mandatory FCoE and FC parameters are correctly configured) or Incomplete (either the FC-MAP value, fabric ID, or VLAN ID are not correctly configured).
<b>Oper-State</b>	Operational status of link to the fabric: Up (link is up and transmitting FC traffic), Down (link is down and not transmitting FC traffic), Link-wait (link is up and waiting for FLOGI to complete on peer FC port), or Removed (port has been shut down).
<b>Members</b>	The switches with the FC Flex IO module Ethernet and FC ports that are members of the dedicated FCoE VLAN that carries storage traffic to the specified fabric.

### Example

```

FTOS#show fcoe-map brief
Fabric-Name Fabric-Id Vlan-Id FC-MAP FCF-Priority Config-State Oper-
State
test 16 16 0efc02 128 ACTIVE UP
cnatest 1003 1003 0efc03 128 ACTIVE UP
sitest 1004 1004 0efc04 128 ACTIVE DOWN

FTOS#show fcoe-map si
Fabric Name si

```

```

Fabric Id      1004
Vlan Id       1004
Vlan priority  3
FC-MAP        0efc04
FKA-ADV-Period 8
Fcf Priority   128
Config-State  ACTIVE
Oper-State    DOWN
Members

```

**Related Commands**

`fcoe-map` — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

## show npiv devices

Display the FCoE and FC devices currently logged in to a Switch with the FC Flex IO module NPIV proxy gateway.

**Syntax** `show npiv devices [brief]`

**Parameters** **brief** Displays an overview of current server CNA-fabric connections over a switch with the FC Flex IO module NPIV proxy gateway.

**Command Modes**

- EXEC
- EXEC Privilege

**Supported Modes** Full-Switch

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.3(0.0)	Introduced on the M I/O Aggregator and MXL 10/40GbE Switch with the FC Flex IO module.

**Usage Information**

Use the `show npiv devices` command to display information on the server CNA, server-facing Ethernet and fabric-facing FC ports, and the SAN fabric in each server-fabric connection over a switch with the FC Flex IO module NPIV proxy gateway.

The following table describes the `show npiv devices brief` output shown in the example below.

Field	Description
<b>ENode-Intf</b>	A switch with the FC Flex IO module Ethernet interface ( <i>slot/port</i> ) to which a server CNA is connected.
<b>ENode-WWPN</b>	Worldwide port name (WWPN) of a server CNA port.
<b>FCoE-Vlan</b>	VLAN ID of the dedicated VLAN used to transmit FCoE traffic to and from the fabric.
<b>Fabric-Intf</b>	Fabric-facing Fibre Channel port ( <i>slot/port</i> ) on which FC traffic is transmitted to the specified fabric.
<b>Fabric-Map</b>	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
<b>LoginMethod</b>	Method used by the server CNA to log in to the fabric; for example: FLOGI - ENode logged in using a fabric login (FLOGI). FDISC - ENode logged in using a fabric discovery (FDISC).
<b>Status</b>	Operational status of the link between a server CNA port and a SAN fabric: Logged In - Server has logged in to the fabric and is able to transmit FCoE traffic.

**Example**

```
Dell# show npiv devices brief
```

```
Total NPIV Devices = 2
-----
```

ENode-Intf	ENode-WWPN	FCoE-Vlan	Fabric-Intf	Fabric-Map	LoginMethod	Status
Te 0/12 LOGGED_IN	20:01:00:10:18:f1:94:20	1003	Fc 0/5	fid_1003	FLOGI	
Te 0/13 LOGGED_IN	10:00:00:00:c9:d9:9c:cb	1003	Fc 0/0	fid_1003	FDISC	

## Usage Information

The following table describes the `show npiv devices` output shown in the example below.

Field	Description
<b>ENode [number]</b>	A server CNA that has successfully logged in to a fabric over a switch with the FC Flex IO module Ethernet port in ENode mode.
<b>ENode MAC</b>	MAC address of a server CNA port.
<b>ENode Intf</b>	Port number of a server-facing Ethernet port operating in ENode mode.
<b>FCF MAC</b>	Fibre Channel forwarder MAC: MAC address of the switch with the FC Flex IO module FCF interface.
<b>Fabric Intf</b>	Fabric-facing Fibre Channel port ( <i>slot/port</i> ) on which FCoE traffic is transmitted to the specified fabric.
<b>FCoE VLAN</b>	ID of the dedicated VLAN used to transmit FCoE traffic from a server CNA to a fabric and configured on both the server-facing the switch with the FC Flex IO module port and server CNA port.
<b>Fabric Map</b>	Name of the FCoE map containing the FCoE/FC configuration parameters for the server CNA-fabric connection.
<b>ENode WWPN</b>	Worldwide port name of the server CNA port.
<b>ENode WWNN</b>	Worldwide node name of the server CNA.
<b>FCoE MAC</b>	Fabric-provided MAC address (FPMA). The FPMA consists of the FC-MAP value in the FCoE map and the FC-ID provided by the fabric after a successful FLOGI. In the FPMA, the most significant bytes are the FC-MAP; the least significant bytes are the FC-ID.
<b>FC-ID</b>	FC port ID provided by the fabric.
<b>LoginMethod</b>	Method used by the server CNA to log in to the fabric; for example, FLOGI or FDISC.
<b>Secs</b>	Number of seconds that the fabric connection is up.
<b>State</b>	Status of the fabric connection: logged in.

## Example

```
ENode[0]:
ENode MAC      : 00:10:18:f1:94:21
ENode Intf     : Te 0/12
FCF MAC        : 5c:f9:dd:ef:10:c8
Fabric Intf    : Fc 0/5
FCoE Vlan      : 1003
Fabric Map     : fid_1003
ENode WWPN     : 20:01:00:10:18:f1:94:20
ENode WWNN     : 20:00:00:10:18:f1:94:21
FCoE MAC       : 0e:fc:03:01:02:01
FC-ID          : 01:02:01
LoginMethod    : FLOGI
Secs           : 5593
Status         : LOGGED_IN

ENode[1]:
ENode MAC      : 00:10:18:f1:94:22
ENode Intf     : Te 0/13
FCF MAC        : 5c:f9:dd:ef:10:c9
Fabric Intf    : Fc 0/0
FCoE Vlan      : 1003
```

```
Fabric Map      :   fid_1003
ENode WWPN     :   10:00:00:00:c9:d9:9c:cb
ENode WWNN     :   10:00:00:00:c9:d9:9c:cd
FCoE MAC       :   0e:fc:03:01:02:02
FC-ID          :   01:02:01
LoginMethod    :   FDISC
Secs           :   5593
Status         :   LOGGED_IN
```

**Related  
Commands**

[fcoe-map](#) — creates an FCoE map which contains the parameters used in the communication between servers and a SAN fabric.

# Debugging and Diagnostics

This chapter contains the following sections:

- [Offline Diagnostic Commands](#)
- [Hardware Commands](#)

## Topics:

- [Offline Diagnostic Commands](#)
- [Hardware Commands](#)
- [clear hardware stack-unit](#)
- [clear hardware system-flow](#)
- [show hardware layer2 acl](#)
- [show hardware layer3](#)
- [diag stack-unit](#)
- [hardware watchdog](#)
- [online stack-unit](#)
- [offline stack-unit](#)
- [show diag](#)
- [show hardware stack-unit](#)
- [show hardware system-flow](#)
- [show hardware buffer interface](#)
- [show hardware counters interface interface](#)
- [show hardware drops](#)

## Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, the Dell Networking OS results are saved as a text file (TestReport-SU-X.txt) in the flash directory. The `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.
- Offline diagnostics cannot be run in Stacking mode.
- 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 via a stacking link.
- Diagnostic results are stored in a file (TestReport-SU-X.txt) in the flash directory. To review the results, use the `show file` command, which prints the results to the screen.
- Diagnostics only test connectivity, not the entire data path.

The offline diagnostics commands are:

- [diag stack-unit](#)
- [offline stack-unit](#)
- [show diag](#)

## Hardware Commands

These commands display information from a hardware sub-component or ASIC.

The hardware commands are:

- [clear hardware stack-unit](#)
- [show diag](#)



- [show hardware stack-unit](#)
- [show hardware system-flow](#)

## clear hardware stack-unit

Clear statistics from selected hardware components.

**Syntax** `clear hardware stack-unit 0-5 {counters | unit 0-1 counters | cpu data-plane statistics | stack-port 9-12}`

<b>Parameters</b>	<p><b>stack-unit 0-5</b> Enter the keywords <code>stack-unit</code> then 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.</p> <p><b>counters</b> Enter the keyword <code>counters</code> to clear the counters on the selected stack member.</p> <p><b>unit 0-0 counters</b> Enter the keyword <code>unit</code> along with a port-pipe number, from 0 to 1, then the keyword <code>counters</code> to clear the counters on the selected port-pipe.</p> <p><b>cpu data-plane statistics</b> Enter the keywords <code>cpu data-plane statistics</code> to clear the data plane statistics.</p> <p><b>stack-port 9-12</b> 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 9 to 12.</p>
-------------------	---

**NOTE:** You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the `show system stack-ports` command.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.

**Related Commands** [show diag](#) — 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 0-5 port-set 0-0 counters`

<b>Parameters</b>	<p><b>stack-unit 0-5</b> Enter the keywords <code>stack-unit</code> then 0 to 5 to select a particular stack member and then enter one of the following command options to clear a specific collection of data.</p> <p><b>port-set 0-0 counters</b> 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.</p>
-------------------	---

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

**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.

## show hardware layer2 acl

Display Layer 2 ACL or eg data for the selected stack member and stack member port-pipe.

<b>Syntax</b>	<code>show hardware layer2 acl stack-unit 0-5 port-set 0-0</code>	
<b>Parameters</b>	<b>stack-unit 0-5</b>	Enter the keyword <code>stack-unit</code> then 0 to 5 to select a stack ID.
	<b>port-set 0-0</b>	Enter the keywords <code>port-set</code> with a port-pipe number.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## show hardware layer3

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

<b>Syntax</b>	<code>show hardware layer3 {acl   qos} stack-unit 0-5 port-set 0-0</code>	
<b>Parameters</b>	<b>acl   qos</b>	Enter either the keyword <code>acl</code> or the keyword <code>qos</code> to select between ACL or QoS data.
	<b>stack-unit 0-5</b>	Enter the keywords <code>stack-unit</code> then a numeral from 0 to 5 to select a stack ID.
	<b>port-set 0-0</b>	Enter the keyword <code>port-set</code> with a port-pipe number.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	Full-Switch	

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## diag stack-unit

Run offline diagnostics on a stack unit.

<b>Syntax</b>	<code>diag stack-unit number {alllevels   level0   level1   level2 [verbose no-reboot]   terminate   interactive test &lt;id&gt;}</code>
---------------	--

<b>Parameters</b>	<b><i>number</i></b>	Enter the stack-unit number. The range is from 0 to 5.
	<b>alllevels</b>	Enter the keyword <code>alllevels</code> to run the complete set of offline diagnostic tests.
	<b>level0</b>	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.
	<b>level1</b>	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.
	<b>level2</b>	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.
	<b>verbose</b>	Enter the keyword <code>verbose</code> to run the diagnostic in Verbose mode. Verbose mode gives more information in the output than Standard mode.
	<b>no-reboot</b>	Enter the keyword <code>no-reboot</code> to avoid automatic rebooting of the chassis after completion of diagnostic execution. Generally, this option is never used because if you run the diagnostic once again without rebooting the chassis, it may cause an issue with the diagnostic results..
	<b>terminate</b>	Enter the keyword <code>terminate</code> to stop the execution of the level diag that is already started using the <code>diag stack-unit</code> command. Once this CLI is issued, syslogs indicating the termination of the diag test is displayed. The diag results for the executed tests are stored in the flash directory ( <code>TestReport-SU-X.txt</code> ).
	<b>interactive</b>	Enter the keyword <code>interactive</code> to run some individual diag tests such as <code>POWERLEDTTEST</code> , <code>STATUSLEDTTEST</code> and so on. The help option under the interactive command displays the list of tests that can be run.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

## hardware watchdog

Set the watchdog timer to trigger a reboot and restart the system.

**Syntax** `hardware watchdog`

**Defaults** Enabled

**Command Modes** • CONFIGURATION

**Supported Modes** All Modes

<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.
<b>Usage Information</b>	This command enables a hardware watchdog mechanism that automatically reboots an Dell Networking OS switch/router with a single unresponsive unit. This is a last resort mechanism intended to prevent a manual power cycle.	

## online stack-unit

Place a stack unit in the online state.

<b>Syntax</b>	<code>online stack-unit <i>number</i></code>	
<b>Parameters</b>	<b><i>number</i></b>	Enter the stack-unit number. The range is from 0 to 5.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>8.3.16.1</b>	Introduced on the MXL 10/40GbE Switch IO Module.

## offline stack-unit

Place a stack unit in the offline state.

<b>Syntax</b>	<code>offline stack-unit <i>number</i></code>	
<b>Parameters</b>	<b><i>number</i></b>	Enter the stack-unit number. The range is from 0 to 5.
<b>Defaults</b>	none	
<b>Command Modes</b>	EXEC Privilege	
<b>Supported Modes</b>	All Modes	
<b>Command History</b>	<b>Version</b>	<b>Description</b>
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.4(0.0)</b>	Supported on the FN I/O Aggregator.
	<b>8.3.17.0</b>	Supported on the M I/O Aggregator.

**Usage Information** While executing the offline stack unit CLI, the following warning message is displayed:

```
Dell#offline stack-unit 0
Warning - offline of unit will bring down all the protocols and
the unit will be operationally down, except for running Diagnostics.
Please make sure that stacking/fanout not configured for Diagnostics
execution.
Also reboot/online command is necessary for normal operation after the
offline command is issued.
Proceed with Offline [confirm yes/no]:no
Dell#
```

Make sure that stacking is not configured for Diagnostics execution. Also, reboot/online command is necessary for normal operation after the offline command is issued.

## show diag

View diagnostics information.

**Syntax** `show diag {information | stack-unit unit-id [detail | summary] | testcase}`

<b>Parameters</b>	<b>information</b>	Enter the keyword <code>information</code> to view current diagnostics information in the system.
	<b>stack-unit <i>unit-id</i></b>	Enter the keyword <code>stack-unit</code> followed by the <i>unit-id</i> to display information on a specific stack member. The range is from 0 to 5.
	<b>detail</b>	(OPTIONAL) Enter the keyword <code>detail</code> to view detailed diagnostics information.
	<b>summary</b>	(OPTIONAL) Enter the keyword <code>summary</code> to view a summary of the diagnostics information. By default, the summary is displayed.
	<b>testcase</b>	Enter the keyword <code>testcase</code> to view the list of all the diag tests available.

**Defaults** Summary

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.4(0.0)	Supported on the FN I/O Aggregator.

**Example 1 (show diag information Command)**

```
Dell#show diag information
Diag information:
Diag software image version:
9-4(0-180)
-----
Stack-unit Member 0: No Unit diags executed yet
(Stackunit not Offline).
Stack-unit Member 1: Not present.
Stack-unit Member 2: Not present.
Stack-unit Member 3: Not present.
Stack-unit Member 4: Not present.
Stack-unit Member 5: Not present.
-----
Dell#
```

**Example 2 (show diag stack-unit Command)**

```
Dell#show diag stackunit 0
Diag status of Stackunit member 0:
-----
Stackunit is currently offline.
Stackunit level0 diag issued at Tue May 15, 2012 11:11:47 AM.
Current diag status: Unit diags are terminated.
Total number of diags:      17
Number of diags performed:  1
Number of diags passed:     1
Number of diags failed:     0
Number of diags pending:   16
Last Test executed:        POWERRAILSTATUSTEST
Last notification received at: Tue May 15, 2012 11:12:24 AM
-----
```

**Example 3  
(show diag  
testcase stack-  
unit Command)**

```
Dell#show diag testcase stack-unit 0
***** Blade IOM Diagnostics Test *****

Test ID Test Description                Test Level
-----
1        POWERRAILSTATUSTEST              Level0
3        TSENSORACCESSTEST                Level0
4        RTCPRESENCETEST                Level0
5        CPUSDRAMPRESENCETEST          Level0
6        CPUSDRAMSIZEEST                Level0
7        USBACCESSTEST                 Level0
8        USBHOSTCONTROLLERACCESSTEST  Level0
9        SDFLASHACCESSTEST             Level0
11       CPLDPRESENCETEST              Level0
12       FLASHACCESSTEST               Level0
13       BOARDREVTEST                  Level0
14       MGMTPHYPRESENCETEST           Level0
16       SFPPLUSPRESENCETEST           Level0
17       CPUTYPEDETECTTEST            Level0
101      RTCFUNCTIONTEST                Level1
102      RTCROLLOVERTEST               Level1
103      GPIOACCESSTEST                Level1
104      PSOCACCESSTEST                Level1
105      PCIEBCM56344ACCESSTEST        Level1
106      CPUSDRAMACCESSTEST            Level1
107      CPUSDRAMDATA LINETEST          Level1
108      CPUSDRAMADDRESS LINETEST      Level1
109      USBFILECOPYTEST                Level1
110      FLASHRWTEST                   Level1
111      I2CSTRESSTEST                  Level1
113      SERVERPORTPHYACCESSTEST       Level1
114      SERVERPORTPHYRWTEST            Level1
117      SFPPLUSPHYEXTLINKTEST          Level1
123      MGMTPHYACCESSTEST              Level1
124      SDFLASHFILECOPYSTRESSTEST     Level1
201      SFPPLUSPHYLNKSPEEDTEST         Level2
203      MGMTPHYLOOPBACKTEST            Level2
204      MGMTMACLOOPBACKTEST            Level2
205      CPUSNAKESERVERPORTPHYLPBKTEST  Level2
206      CPUSNAKESERVERPORTMACLPBKTEST  Level2
207      CPUSNAKESFPPHYLPBKTEST         Level2
208      CPUSNAKESFPPMACLPBKTEST        Level2

tal Diagnostic Testcases in All Levels: 37

***** END *****

Dell#
```

**Example 4  
(show diag  
testcase stack-  
unit interactive  
Command)**

```
Dell#show diag testcase stack-unit 0 interactive
***** Blade IOM Diagnostics Test *****

Test ID Test Description                Test Level
-----
401      POWERLEDTEST                  Interactive
402      DEBUGLEDTEST                  Interactive
403      STATUSLEDTEST                  Interactive
406      RTCBATTERYTEST                 Interactive
407      CPLDRESETTEST                  Interactive
408      I2CDEVICESCANTEST               Interactive
409      SERVERPORTPHYEXTLINKTEST        Interactive
410      CPUSNAKESFPPEXTLPBKTEST         Interactive

Total Diagnostic Testcases in Interactive: 8

***** END *****
```

## 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

```
show hardware stack-unit 0 {buffer [ unit 0 ] total buffer | buffer unit 0
interface all queue [(0-14) | all] buffer-info} {cpu {data-plane statistics
| management statistics | private-mgmt statistics} | drops [unit 0-0 | fpga
registers | fru dump | stack-port 9-12 | unit 0-0 {counters | details |
ipmc-replication | port-stats [detail] | register | table-dump WORD}}
```

### Parameters

<b>stack-unit 0 {command-option}</b>	Enter the keywords <code>stack-unit</code> then 0 to select the stack member and then enter one of the following command options to display a collection of data based on the option entered.
<b>buffer</b>	Enter the keyword <code>buffer</code> . To display buffer statistics for a all interface, enter the keyword <code>interface</code> followed by the keyword <code>all</code> . To display the forwarding plane statistics containing the packet buffer usage per port per stack unit, enter the keyword <code>unit</code> then 0 for port-pipe 0, then <code>port</code> and the port number (42-53, and then <code>buffer-info</code> .
<b>cpu {data-plane statistics   management statistics   private-mgmt statistics}</b>	Enter the keyword <code>cpu</code> then one of the keywords to display the CPU statistics: <code>data-plane statistics</code> , <code>management statistics</code> , or <code>private-mgmt statistics</code> .
<b>drops interface interface</b>	Enter the keyword <code>drops</code> to display internal drops on the selected stack member.
<b>fpga registers</b>	Enter the keywords <code>fpga registers</code> to display fpga details.
<b>fru dump</b>	Enter the keywords <code>fru dump</code> to display fru details.
<b>stack-port 9-12</b>	Enter the keywords <code>stack-port</code> and a stacking port number to select a stacking port for which to display statistics. Identify the stack port number as you would to identify a 10G port that was in the same place in one of the rear modules. <b>NOTE:</b> You can identify stack port numbers by physical inspection of the rear modules. The numbering is the same as for the 10G ports. You can also inspect the output of the <code>show system stack-ports</code> command.
<b>unit 0-0 {counters   details   ipmc-replication   port-stats [detail]   register   table-dump WORD}</b>	Enter the keyword <code>unit</code> then 0 for port-pipe 0, 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: <code>counters</code> , <code>details</code> , <code>ipmc-replication</code> , <code>port-stats [detail]</code> , <code>register</code> , or <code>table-dump WORD</code> .

### Defaults

none

### Command Modes

- EXEC
- EXEC Privilege

### Supported Modes

All Modes

**Command History**

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Replaced the keyword port with interface.
9.4(0.0)	Supported on the FN I/O Aggregator.

**Example (data-plane)**

```
Dell#show hardware stack-unit 0 cpu data-plane statistics

bc pci driver statistics for device:
 rxHandle           :9798
 noMhdr             :0
 noMbuf             :0
 noClus             :0
 recvd              :9798
 dropped            :0
 recvToNet          :9778
 rxError            :0
 rxDatapathErr     :0
 rxPkt(COS0)       :0
 rxPkt(COS1)       :0
 rxPkt(COS2)       :25
 rxPkt(COS3)       :0
 rxPkt(COS4)       :0
 rxPkt(COS5)       :0
 rxPkt(COS6)       :0
 rxPkt(COS7)       :226
 rxPkt(COS8)       :9527
 rxPkt(COS9)       :0
 rxPkt(COS10)      :0
 rxPkt(COS11)      :20
 rxPkt(UNIT0)      :9798
 transmitted        :4353
 txRequested        :4353
 noTxDesc           :0
 txError            :0
 txReqTooLarge     :0
 txInternalError   :0
 txDatapathErr     :0
 txPkt(COS0)       :0
 txPkt(COS1)       :0
 txPkt(COS2)       :0
 txPkt(COS3)       :0
 txPkt(COS4)       :0
 txPkt(COS5)       :0
 txPkt(COS6)       :0
 txPkt(COS7)       :0
 txPkt(COS8)       :0
 txPkt(COS9)       :0
 txPkt(COS10)      :0
 txPkt(COS11)      :0
 txPkt(UNIT0)      :0
Dell#
```

**Example**

```
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 (drop counters)**

```
Dell#show hardware stack-unit 1 unit 0 counters
unit: 0 port: 1 (interface Te 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)
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 (port-statistics)**

```

Dell#show hardware stack-unit 0 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
11996 xe0 up 10G FD SW Yes Forward None FA KR
11996 xe1 up 10G FD SW Yes Forward None FA KR
11996 xe2 up 10G FD SW Yes Forward None FA KR
11996 xe3 down 1G FD SW Yes Block RX None FA GMII
11996 xe4 up 10G FD SW Yes Forward None FA KR
11996 xe5 down 1G FD SW Yes Block RX None FA GMII
11996 xe6 up 10G FD SW Yes Forward None FA KR

```

```

11996
11996   xe7  down  1G FD  SW  Yes  Block  RX  None  FA  GMII
11996   xe8  down  10G FD SW  No   Block  RX  None  FA  SFI
11996   xe9  down  10G FD SW  No   Block  RX  None  FA  SFI
11996   xe10 up    10G FD SW  No   Forward      None  FA  SFI
11996   xe11 up    10G FD SW  No   Forward      None  FA  SFI
11996
Dell#

```

**Example (register)**

```

Dell#show hardware stack-unit 0 unit 0 register
0x0f180d34 ALTERNATE_EMIRROR_BITMAP_PARITY_CONTROL.ipipe0 = 0x00000001
0x0f180d35 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_INTR.ipipe0 =
0x00000000
0x0f180d36 ALTERNATE_EMIRROR_BITMAP_PARITY_STATUS_NACK.ipipe0 =
0x00000000
0x0018070c ARB_EOP_DEBUG.ipipe0 = 0x00000000
0x00180312 ARB_RAM_DBGCTRL.ipipe0 = 0x00000000
0x03300000 ASF_PORT_SPEED.cpu0 = 0x00000000
0x03322000 ASF_PORT_SPEED.xe0 = 0x00000000
0x03326000 ASF_PORT_SPEED.xe1 = 0x00000000
0x0332a000 ASF_PORT_SPEED.xe2 = 0x00000007
0x0332e000 ASF_PORT_SPEED.xe3 = 0x00000000
0x03323000 ASF_PORT_SPEED.xe4 = 0x00000000
0x03327000 ASF_PORT_SPEED.xe5 = 0x00000000
0x0332b000 ASF_PORT_SPEED.xe6 = 0x00000000
0x0332f000 ASF_PORT_SPEED.xe7 = 0x00000000
0x03324000 ASF_PORT_SPEED.xe8 = 0x00000000
0x03328000 ASF_PORT_SPEED.xe9 = 0x00000000
0x0332c000 ASF_PORT_SPEED.xe10 = 0x00000000
0x03330000 ASF_PORT_SPEED.xe11 = 0x00000000
0x03325000 ASF_PORT_SPEED.xe12 = 0x00000000
0x03329000 ASF_PORT_SPEED.xe13 = 0x00000000
0x0332d000 ASF_PORT_SPEED.xe14 = 0x00000000
0x03331000 ASF_PORT_SPEED.xe15 = 0x00000000
0x03332000 ASF_PORT_SPEED.xe16 = 0x00000000
0x03336000 ASF_PORT_SPEED.xe17 = 0x00000000
0x0333a000 ASF_PORT_SPEED.xe18 = 0x00000000
0x0333e000 ASF_PORT_SPEED.xe19 = 0x00000000
0x03333000 ASF_PORT_SPEED.xe20 = 0x00000000
0x03337000 ASF_PORT_SPEED.xe21 = 0x00000000
0x0333b000 ASF_PORT_SPEED.xe22 = 0x00000000
0x0333f000 ASF_PORT_SPEED.xe23 = 0x00000000
0x03334000 ASF_PORT_SPEED.xe24 = 0x00000000
0x03338000 ASF_PORT_SPEED.xe25 = 0x00000000
0x0333c000 ASF_PORT_SPEED.xe26 = 0x00000000
0x03340000 ASF_PORT_SPEED.xe27 = 0x00000000
0x03335000 ASF_PORT_SPEED.xe28 = 0x00000000
0x03339000 ASF_PORT_SPEED.xe29 = 0x00000000
!----- output truncated -----!

```

**Example (unit details)**

```

Dell#show hardware stack-unit 0 unit 0 details
*****

The total no of FP & CSF Devices in the Card is 1
The total no of FP Devices in the Card is 1
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 12
The number of Hg ports in devices 0 is - -1
The CPU Port of the device is 0
The starting unit no the SWF in the device is 0
*****

bcmLinkMonStatusShow: The Current Link Status Is

```

```
Front End Link Status      0xea30000000000000000000000000000000
Front End Port Present Status 0x00000000000000000000000000000000
Back Plane Link Status    0x00000000
```

```
*****
```

```
Link Status of all the ports in the Device - 0
```

```
The linkStatus of Front End Port 42 is TRUE
The linkStatus of Front End Port 43 is TRUE
The linkStatus of Front End Port 44 is TRUE
The linkStatus of Front End Port 45 is FALSE
The linkStatus of Front End Port 46 is TRUE
The linkStatus of Front End Port 47 is FALSE
The linkStatus of Front End Port 48 is TRUE
The linkStatus of Front End Port 49 is FALSE
The linkStatus of Front End Port 50 is FALSE
The linkStatus of Front End Port 51 is FALSE
The linkStatus of Front End Port 52 is TRUE
The linkStatus of Front End Port 53 is TRUE
*****
```

```
*****
```

```
ModPort Table for Device - 0
For Destination Mod Id 0 Destination Port is 0
*****
Dell#
```

**Example (Buffer-Info)**

```
Dell# show hardware stack-unit 1 buffer unit 0 port 1 priority-group 0
buffer-info

----- Buffer Accounting Stats for Unit 0 Port 1 priority-group 0 -----
Maximum Shared Limit: 0
Default Packet Buffer allocate for the priority-group: 61440
Accounted Packet Buffer: 0
```

**Example (buffer)**

```
Dell#show hardware stack-unit 0 buffer total-buffer
----- Buffer Details for Stack-Unit 0 -----
Total Buffers allocated per Stack-Unit 19456
Dell#
```

**Example (Queue2/Buffer-Info)**

```
Dell#show hardware stack-unit 1 buffer unit 0 interface all queue 6
buffer-info
      Buffer Stats for Front End Ports
      =====
----- Buffer Stats for Interface Te 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 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 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 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 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 Queue 6 -----
Maximum Shared Limit: 7667
```

```
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
<output truncated for brevity>
```

**Related Commands**

- [show interfaces stack-unit](#) — displays information on all interfaces on a specific stack member.
- [show processes cpu](#) — displays CPU usage information based on running processes.
- [show system](#) — displays the current status of all stack members or a specific member.

## show hardware system-flow

Display Layer 2 ACL or QoS data for the selected stack member and stack member port-pipe.

**Syntax** `show hardware system-flow layer2 stack-unit 0-5 port-set 0-0 [counters]`

- 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 0-5** Enter the keywords `stack-unit` then 0 to 5 to select a stack member ID.
  - port-set 0-0 [counters]** Enter the keywords `port-set` with a port-pipe number—0.  
(OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

**Defaults** none

**Command Modes** EXEC Privilege

**Supported Modes** All Modes

Command History	Version	Description
	9.9(0.0)	Introduced on the FN IOM.
	9.4(0.0)	Supported on the FN I/O Aggregator.

**Example**

```
Dell#show hardware system-flow layer2 stack-unit 0 port-set 0 counters
```

EntryId	Description	#HITS
767	LLDP BPDU Redirects	2611
765	LACP traffic Redirects	250
763	ARP Reply Redirects	0
762	Slow Protocol Drops	1155
758	OSPFv3 Multicast [33:33:00:00:00:06]	0
759	OSPFv3 Multicast [33:33:00:00:00:05]	0
756	GRAT ARP	0
711	VLT ARP Replies for Peer	0
710	ICL Hellos	0
709	ICL MAC SYNC Frames	0
708	VLT STP BPDUs Tunneled	0
707	VLT IGMP Sync Frames	0
706	VLT ARP Replies Tunneled	0
705	VLT L2PM Sync Frames	0
704	VLT ARP Sync Frames	0
703	VLT IPM Sync Frames	0
701	VLT NDPM Sync Frames	0
699	VLT TTL1 Packets Tunneled	0
698	VLT Dyn Client pkts	0
697	VLT PIM Sync Frames	0
696	VLT MRTM Sync Frames	0
695	VLT SMUX Sync Frames	0
693	DROP Cases	0
509	BGP_SPORT PACKETS	0
508	BGP_DPORT PACKETS	0

```

507      MSDP_SPORT PACKETS          0
506      MSDP_DPORT PACKETS         0
510      IGMP_PACKETS WITH IP OPTIONS 26
505      FP Entry for OSPF IPv4 Unicast 0
504      FP Entry for RIP IPv4 Unicast 0
503      FP Entry for OSPF IPv6 Unicast 0
502      FP Entry for NA IPv6         0
501      FP Entry for RA IPv6         0
500      FP Entry for NS IPv6         4
499      FP Entry for RS IPv6         8
498      FP Entry for MLD IPv6        0
497      L3 CPU Bound Traffic
        ClassId 2 to Q5              0
496      FP Entry for ICMP CPU Terminated IPv6 0
495      FP Entry for ICMP IPv6       0
494      L3 Term Traffic
        ClassID 1 to Q6              0
493      Unknown MCAST Packets        0
492      224.0.0.x                    24
491      224.0.1.1                    0
490      SIMPLEMUX - VLAN Flood
        Restrict Entry                0
249      IGMP Packets                 26
147      MULTICAST KNOWN TTL1          0
145      L2_DST_HIT+BC MAC+VLAN 4095  0
144      L2_DST_HIT+BC MAC            0
773      Known & Unknown L3UC Packets 0
772      Unknown L2MC Packets         26
771      Known and Unknown L3MC Packets 0
770      L2UCAST + L2DLF Packets      0
769      L2BCASTPackets               0
Dell#

```

### Example (non-counters)

```

Dell#show hardware system-flow layer2 stack-unit 0 port-set 0

##### FP Entry for redirecting STP BPDU to CPU Port #####
EID 2048: gid=1,
        slice=15, slice_idx=0x00, prio=0x800, flags=0x82, Installed
        tcam: color_indep=0, higig=0, higig_mask=0,
        KEY=0x00000000 00000000 00000000 0180c200 00000000 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=0, mode=0x01, entries=1}

##### FP Entry for redirecting LLDP BPDU to RSM #####
EID 2047: gid=1,
        slice=15, slice_idx=0x01, prio=0x7ff, flags=0x82, Installed
        tcam: color_indep=0, higig=0, higig_mask=0,
        KEY=0x00000000 00000000 00000000 0180c200 000e0000 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=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 buffer interface

Display buffer statistics for a specific interface.

**Syntax** `show hardware buffer interface interface{priority-group { id | all } | queue { id| all} ] buffer-info`

<b>Parameters</b>	<p><b>interface</b> <b><i>interface</i></b> Enter any of the following keywords and slot/port or number information:</p> <ul style="list-style-type: none"> <li>For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information.</li> </ul> <p><b>priority-group</b> Identifier of the priority group in the range of 0 to 7.</p> <p><b>queue</b> Enter the keyword <code>queue</code> followed by <i>id</i> for specific queue or keyword <code>all</code>.</p> <p><b>buffer-info</b> To display total buffer information for the interface, enter the keywords <code>buffer-info</code>.</p>
-------------------	--

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Introduced on the M I/O Aggregator and FN I/O Aggregator.

### Example displaying total-buffer information for the interface

```

Dell# show hardware buffer interface tengigabitethernet 1/1 buffer-info
----- Buffer Stats for Interface Te 1/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0

```



**Example displaying priority-group range**

```
Dell#show hardware buffer interface tengigabitethernet 1/1 priority-group 0
buffer-info
----- Buffer stats for unit: 0 port: 1 (interface Te 1/1) -----
-----
PG# PRIORITIES          MIN      ALLOTTED (CELLS)  COUNTER (CELLS)
          SHARED  MODE   HDRM      MIN      SHARED  HDRM
-----
0   -                61440  0          STATIC  174      0       0       0
-----
Dell#
```

**Example displaying queue range**

```
Dell#show hardware buffer interface tengigabitethernet 1/1 queue all buffer-info
----- Buffer Stats for Interface Te 1/1 Queue 0 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 1 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 2 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 3 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 4 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 5 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 6 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 7 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 8 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 9 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 10 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1 Queue 11 -----
Maximum Shared Limit: 29514
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
-----
<output truncated for brevity>
```

## show hardware counters interface *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 or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

**Defaults** none

- Command Modes**
- EXEC
  - EXEC Privilege

**Supported Modes** Full-Switch

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

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

Version	Description
9.9(0.0)	Introduced on the FN IOM.
9.8(0.0)	Introduced on the FN I/O Aggregator.

**Example**

```
Dell#show hardware counters interfac tengigabitethernet 5/1
unit: 0 port: 2 (interface Te 5/1)
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 or slot/port-range or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

**drops** Enter the keyword `drops` to display internal drops.

**Command Modes** EXEC  
EXEC Privilege

**Supported Modes** Full-Switch

Command History	Version	Description
	<b>9.9(0.0)</b>	Introduced on the FN IOM.
	<b>9.8(0.0)</b>	Introduced on the M I/O Aggregator and the FN I/O Aggregator.

### Example displaying internal drops for the specific interface

```
Dell#show hardware drops interface tengigabitethernet 2/1

Drops in Interface Te 2/1:
--- Ingress Drops ---
Ingress Drops : 0
IBP CBP Full Drops : 0
PortSTPnotFwd Drops : 0
IPv4 L3 Discards : 0
Policy Discards : 0
Packets dropped by FP (L2+L3) Drops : 0
Port bitmap zero Drops : 0
Rx VLAN Drops : 0
--- Ingress MAC counters---
Ingress FCSDrops : 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

```

**Example  
displaying  
internal drops for  
FC port**

```

Dell(conf)#do show hardware drops interface fibreChannel 0/49
Drops in Interface Fc 0/49:
  --- Ingress Drops ---
Ingress Drops          : 10
IBP CBP Full Drops     : 0
PortSTPnotFwd Drops   : 0
IPv4 L3 Discards       : 0
Policy Discards        : 0
Packets dropped by FP  : 10
(L2+L3) Drops          : 0
Port bitmap zero Drops : 1
Rx VLAN Drops          : 1
  --- Ingress MAC counters---
Ingress FCS Drops      : 0
Ingress MTUExceeds    : 0
  --- MMU Drops ---
Ingress MMU Drops      : 0
Ingress Drops Bytes    : 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
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
Dell(conf)#
```

# Internet Control Message Protocol (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.

**Table 7. ICMP messages and their definitions**

Symbol	Type	Code	Description	Query	Error
.			Timeout (no reply)		
!	0	3	echo reply	.	
U	3		destination unreachable:		
		0	network unreachable		.
		1	host unreachable		.
		2	protocol unreachable		.
		3	port unreachable		.
		4	fragmentation needed but don't fragment bit set		.
		5	source route failed		.
		6	destination network unknown		.
		7	destination host unknown		.
		8	source host isolated (obsolete)		.
		9	destination network administratively prohibited		.
		10	destination host administratively prohibited		.
		11	network unreachable for TOS		.
		12	host unreachable for TOS		.
		13	communication administratively prohibited by filtering		.
		14	host precedence violation		.
		15	precedence cutoff in effect		.
C	4	0	source quench		.
	5		redirect		.
		0	redirect for network		.
		1	redirect for host		.
		2	redirect for type-of-service and network		.
		3	redirect for type-of-service and host		.
	8	0	echo request	.	
	9	0	router advertisement	.	

**Table 7. ICMP messages and their definitions (continued)**

Symbol	Type	Code	Description	Query	Error
	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	.	