9.10(0.0)
Notes, cautions, and warnings

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

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

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

1 About this Guide

- Objectives.......................................................................................................................... 39
- Audience................................................................................................................................. 39
- Conventions............................................................................................................................ 39
- Information Icons.................................................................................................................... 40

2 CLI Basics

- Accessing the Command Line................................................................................................ 41
- Multiple Configuration Users................................................................................................ 41
- Obtaining Help....................................................................................................................... 42
- Navigating the CLI................................................................................................................ 43
- Using the Keyword no Command......................................................................................... 44
- Filtering show Commands..................................................................................................... 44
- Enabling Software Features on Devices Using a Command Option.................................... 45
  - feature vrf.......................................................................................................................... 45
  - show feature...................................................................................................................... 46
- Command Modes.................................................................................................................. 47

3 File Management

- boot system........................................................................................................................... 56
- cd........................................................................................................................................ 58
- copy..................................................................................................................................... 58
- delete................................................................................................................................... 61
- dir........................................................................................................................................ 62
- format................................................................................................................................... 63
- fsck flash............................................................................................................................... 64
- mkdir.................................................................................................................................... 64
- mount nfs............................................................................................................................... 65
- rmdir..................................................................................................................................... 66
- upgrade system.................................................................................................................... 66
- HTTP Copy via CLI............................................................................................................... 68
- rename.................................................................................................................................. 68
- restore factory-defaults....................................................................................................... 69
- show boot system.................................................................................................................. 71
- show bootvar....................................................................................................................... 72
- show file-systems................................................................................................................ 73
- show os-version................................................................................................................... 74
- show running-­config............................................................................................................ 75
- show startup-config............................................................................................................ 79
- show version......................................................................................................................... 80
- upgrade................................................................................................................................. 81

4 Control and Monitoring........................................................................................................ 83

...
show processes cpu
show processes ipc flow-control
show processes memory
show software ifm
show system
show tech-support
ssh-peer-stack-unit
telnet
telnet-peer-stack-unit
terminal length
traceroute
undebug all
virtual-ip
write

5 802.1X

dot1x

dot1x auth-fail-vlan
dot1x auth-server
dot1x auth-type mab-only
dot1x authentication (Configuration)
dot1x authentication (Interface)
dot1x critical-vlan
dot1x guest-vlan
dot1x host-mode
dot1x mac-auth-bypass
dot1x max-eap-req
dot1x max-suppliants
dot1x port-control
dot1x profile
dot1x quiet-period
dot1x reauthentication
dot1x reauth-max
dot1x server-timeout
dot1x static-mab
dot1x supplicant-timeout
dot1x tx-period
mac
show dot1x cos-mapping interface
show dot1x interface
show dot1x profile

6 Access Control Lists (ACL)

Commands Common to all ACL Types
remark
show config
Common IP ACL Commands
access-class................................................................................................................................. 178
clear counters ip access-group..................................................................................................... 180
ip access-group.............................................................................................................................. 180
ip control-plane egress-filter........................................................................................................ 182
show ip accounting access-list...................................................................................................... 182
show ip access-lists......................................................................................................................... 184
Standard IP ACL Commands............................................................................................................. 184
deny........................................................................................................................................................ 185
ip access-list standard....................................................................................................................... 186
permit..................................................................................................................................................... 187
resequence access-list....................................................................................................................... 188
seq.......................................................................................................................................................... 189
Extended IP ACL Commands............................................................................................................... 191
deny........................................................................................................................................................ 191
deny icmp................................................................................................................................................. 193
deny tcp.................................................................................................................................................. 194
deny udp.................................................................................................................................................. 197
ip access-list extended....................................................................................................................... 199
permit..................................................................................................................................................... 200
permit tcp............................................................................................................................................... 202
permit udp............................................................................................................................................ 204
resequence access-list....................................................................................................................... 207
seq.......................................................................................................................................................... 208
Common MAC Access List Commands.............................................................................................. 210
clear counters mac access-group....................................................................................................... 210
mac access-group............................................................................................................................... 211
show mac access-lists........................................................................................................................ 212
show mac accounting access-list.................................................................................................... 213
Standard MAC ACL Commands......................................................................................................... 214
deny........................................................................................................................................................ 214
mac access-list standard.................................................................................................................... 216
permit..................................................................................................................................................... 217
seq.......................................................................................................................................................... 218
Extended MAC ACL Commands........................................................................................................ 219
deny........................................................................................................................................................ 220
mac access-list extended.................................................................................................................... 221
permit..................................................................................................................................................... 223
IP Prefix List Commands.................................................................................................................... 224
clear ip prefix-list............................................................................................................................... 224
deny........................................................................................................................................................ 225
ip prefix-list.......................................................................................................................................... 226
seq.......................................................................................................................................................... 227
show config........................................................................................................................................... 228
show ip prefix-list detail..................................................................................................................... 229
show ip prefix-list summary............................................................................................................... 230
Route Map Commands...................................................................................................................... 231
continue................................................................................................................................................. 231
description................................................................................................................................. 232
match as-path...................................................................................................................................... 233
match community................................................................................................................................... 234
match interface...................................................................................................................................... 234
match ip address.................................................................................................................................... 236
match ip next-hop................................................................................................................................... 237
match ip route-source.......................................................................................................................... 238
match metric............................................................................................................................................ 239
match origin.............................................................................................................................................. 239
match route-type..................................................................................................................................... 240
match tag.................................................................................................................................................. 241
route-map.................................................................................................................................................. 242
set as-path............................................................................................................................................... 243
set automatic-tag..................................................................................................................................... 244
set comm-list delete................................................................................................................................ 245
set community.......................................................................................................................................... 246
set level.................................................................................................................................................... 247
set local-preference.............................................................................................................................. 248
set metric................................................................................................................................................ 249
set metric-type........................................................................................................................................ 250
set next-hop.......................................................................................................................................... 251
set origin.................................................................................................................................................. 252
set tag...................................................................................................................................................... 253
set weight............................................................................................................................................... 254
show config............................................................................................................................................ 254
show route-map...................................................................................................................................... 255
AS-Path Commands................................................................................................................................ 256
ip as-path access-list.............................................................................................................................. 256
show ip as-path-access-lists.................................................................................................................. 257
IP Community List Commands.............................................................................................................. 258
ip community-list.................................................................................................................................... 258
show ip community-lists.......................................................................................................................... 258
deny (for Standard IP ACLs).................................................................................................................. 259
deny (for Extended IP ACLs).................................................................................................................. 260
seq (for Standard IPv4 ACLs)................................................................................................................... 262
deny tcp (for Extended IP ACLs)........................................................................................................... 263
deny udp (for Extended IP ACLs)........................................................................................................... 264
deny arp (for Extended MAC ACLs)....................................................................................................... 265
deny icmp (for Extended IP ACLs)......................................................................................................... 267
deny ether-type (for Extended MAC ACLs)............................................................................................ 268
deny (for Standard MAC ACLs)............................................................................................................. 269
deny (for Extended MAC ACLs)............................................................................................................. 271
permit (for Standard IP ACLs)................................................................................................................ 272
permit arp (for Extended MAC ACLs).................................................................................................... 273
permit ether-type (for Extended MAC ACLs).......................................................................................... 275
permit icmp (for Extended IP ACLs)...................................................................................................... 276
permit udp (for Extended IP ACLs)....................................................................................................... 277
7 Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM) ................................................................. 301
member vlan........................................................................................................................................................................ 301
ip access-group.......................................................................................................................................................... 302
show acl-vlan-group...................................................................................................................................................... 302
show cam-acl-vlan...................................................................................................................................................... 303
cam-acl-vlan.......................................................................................................................................................... 304
show cam-usage........................................................................................................................................................ 305
show running config acl-vlan-group................................................................................................................................. 307
cam-acl-vlan-group...................................................................................................................................................... 308
show acl-vlan-group detail.................................................................................................................................................. 309
description (ACL VLAN Group)................................................................................................................................................ 310

8 Bidirectional Forwarding Detection (BFD) ............................................................................................................................ 311
bfd all-neighbors........................................................................................................................................................ 311
bfd disable................................................................................................................................................................. 313
bfd enable (Configuration)................................................................................................................................................ 313
bfd enable (Interface).................................................................................................................................................. 314
bfd interval .................................................................................................................................................................. 314
bfd neighbor.............................................................................................................................................................. 315
bfd protocol-liveness.................................................................................................................................................... 316
ip route bfd.................................................................................................................................................................. 316
ipv6 ospf bfd all-neighbors............................................................................................................................................ 317
isis bfd all-neighbors.................................................................................................................................................. 318
neighbor bfd.............................................................................................................................................................. 320
neighbor bfd disable.................................................................................................................................................. 320
show bfd neighbors.................................................................................................................................................... 321
vrpm bfd neighbor...................................................................................................................................................... 323

9 Border Gateway Protocol.................................................................................................................................................... 324
BGP IPv4 Commands.................................................................................................................................................... 324
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp summary</td>
<td>368</td>
</tr>
<tr>
<td>show ip bgp paths community</td>
<td>369</td>
</tr>
<tr>
<td>show ip bgp next-hop</td>
<td>370</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>371</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>372</td>
</tr>
<tr>
<td>show ip bgp detail</td>
<td>373</td>
</tr>
<tr>
<td>set extcommunity bandwidth</td>
<td>374</td>
</tr>
<tr>
<td>redistribute ospf</td>
<td>375</td>
</tr>
<tr>
<td>neighbor local-as</td>
<td>376</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>377</td>
</tr>
<tr>
<td>neighbor remove-private-as</td>
<td>378</td>
</tr>
<tr>
<td>neighbor route-map</td>
<td>379</td>
</tr>
<tr>
<td>neighbor route-reflector-client</td>
<td>380</td>
</tr>
<tr>
<td>neighbor sender-side-loopdetect</td>
<td>381</td>
</tr>
<tr>
<td>neighbor send-community</td>
<td>382</td>
</tr>
<tr>
<td>neighbor shutdown</td>
<td>383</td>
</tr>
<tr>
<td>neighbor soft-reconfiguration inbound</td>
<td>384</td>
</tr>
<tr>
<td>neighbor timers</td>
<td>385</td>
</tr>
<tr>
<td>neighbor update-source</td>
<td>386</td>
</tr>
<tr>
<td>neighbor weight</td>
<td>387</td>
</tr>
<tr>
<td>network</td>
<td>388</td>
</tr>
<tr>
<td>network backdoor</td>
<td>389</td>
</tr>
<tr>
<td>permit bandwidth</td>
<td>390</td>
</tr>
<tr>
<td>redistribute</td>
<td>391</td>
</tr>
<tr>
<td>redistribute ospf</td>
<td>392</td>
</tr>
<tr>
<td>router bgp</td>
<td>393</td>
</tr>
<tr>
<td>set extcommunity bandwidth</td>
<td>394</td>
</tr>
<tr>
<td>show capture bgp-pdu neighbor</td>
<td>395</td>
</tr>
<tr>
<td>show config</td>
<td>396</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>397</td>
</tr>
<tr>
<td>show ip bgp cluster-list</td>
<td>398</td>
</tr>
<tr>
<td>show ip bgp community</td>
<td>399</td>
</tr>
<tr>
<td>show ip bgp community-list</td>
<td>400</td>
</tr>
<tr>
<td>show ip bgp dampened-paths</td>
<td>401</td>
</tr>
<tr>
<td>show ip bgp detail</td>
<td>402</td>
</tr>
<tr>
<td>show ip bgp extcommunity-list</td>
<td>403</td>
</tr>
<tr>
<td>show ip bgp filter-list</td>
<td>404</td>
</tr>
<tr>
<td>show ip bgp flap-statistics</td>
<td>405</td>
</tr>
<tr>
<td>show ip bgp inconsistent-as</td>
<td>406</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>407</td>
</tr>
<tr>
<td>show ip bgp next-hop</td>
<td>408</td>
</tr>
<tr>
<td>show ip bgp paths</td>
<td>409</td>
</tr>
<tr>
<td>show ip bgp paths community</td>
<td>410</td>
</tr>
<tr>
<td>show ip bgp peer-group</td>
<td>411</td>
</tr>
<tr>
<td>show ip bgp regexp</td>
<td>412</td>
</tr>
<tr>
<td>show ip bgp summary</td>
<td>413</td>
</tr>
</tbody>
</table>
show running-config bgp................................................................. 427
  timers bgp .............................................................................. 428
MBGP Commands........................................................................ 428
deb ug ip bgp dampening........................................................... 429
distance bgp.............................................................................. 430
  show ip bgp dampened-paths.................................................. 431
BGP Extended Communities (RFC 4360).................................... 432
  set extcommunity rt.............................................................. 432
  set extcommunity soo.......................................................... 433
  show ip bgp paths extcommunity.......................................... 434
  show ip extcommunity-list.................................................... 435
IPv6 BGP Commands.................................................................. 436
  clear ip bgp ipv6 unicast soft................................................ 436
debug ip bgp ipv6 unicast soft-reconfiguration.......................... 437
  ipv6 prefix-list........................................................................ 438
  neighbor soft-reconfiguration inbound.................................... 439
  show ipv6 prefix-list.............................................................. 439
IPv6 MBGP Commands.............................................................. 440
  show ipv6 mbgroutes.............................................................. 440

10 Content Addressable Memory (CAM)...................................... 442
  CAM Profile Commands.......................................................... 442
    cam-acl (Configuration)...................................................... 443
cam-acl-egress........................................................................ 446
cam-optimization.................................................................... 446
  show cam-acl......................................................................... 447
test cam-usage....................................................................... 449

11 Control Plane Policing (CoPP)................................................ 451
  control-plane-cpuqos............................................................ 451
  service-policy rate-limit-cpu-queues..................................... 452
  service-policy rate-limit-protocols........................................ 452
  ip unknown-unicast............................................................. 453
ipv6 unknown-unicast............................................................. 454
  show cpu-queue rate cp......................................................... 455
  show ip protocol-queue-mapping......................................... 456
  show ipv6 protocol-queue-mapping....................................... 457
  show mac protocol-queue-mapping....................................... 457

12 Debugging and Diagnostics.................................................... 459
  Diagnostics and Monitoring Commands.................................. 459
    logging coredump stack-unit............................................... 459
Offline Diagnostic Commands.................................................. 460
  diag stack-unit...................................................................... 460
  offline stack-unit............................................................... 461
  online stack-unit............................................................... 462
  Hardware Commands............................................................ 463
clear hardware stack-unit..................................................................................................................... 463
clear hardware system-flow.................................................................................................................... 464
clear hardware vlan-counters.................................................................................................................. 465
hardware watchdog................................................................................................................................. 465
show hardware mac................................................................................................................................. 466
show hardware ip....................................................................................................................................... 466
show hardware stack-unit.......................................................................................................................... 467
show hardware buffer interface.............................................................................................................. 475
show hardware counters interface......................................................................................................... 476
show hardware buffer-stats-snapshot...................................................................................................... 478
show hardware stack-unit buffer-stats-snapshot (Total Buffer Information)............................................. 479
show hardware system-flow..................................................................................................................... 481
show hardware vlan-counters.................................................................................................................. 482
show hardware drops............................................................................................................................... 483

13 Dynamic Host Configuration Protocol (DHCP).................................................................................. 486

Commands to Configure the System to be a DHCP Server......................................................................... 486
clear ip dhcp........................................................................................................................................... 486
debug ip dhcp server................................................................................................................................. 487
debug ipv6 dhcp....................................................................................................................................... 488
default-router.......................................................................................................................................... 488
disable..................................................................................................................................................... 489
dns-server............................................................................................................................................... 490
domain-name.......................................................................................................................................... 490
excluded-address..................................................................................................................................... 491
hardware-address................................................................................................................................. 492
host......................................................................................................................................................... 492
lease....................................................................................................................................................... 493
netbios-name-server............................................................................................................................... 494
netbios-node-type.................................................................................................................................. 495
network................................................................................................................................................ 495
pool....................................................................................................................................................... 496
show ip dhcp binding............................................................................................................................... 497
show ip dhcp configuration..................................................................................................................... 497
show ip dhcp conflict............................................................................................................................... 498
show ip dhcp server............................................................................................................................... 499

Commands to Configure Secure DHCP................................................................................................. 500
arp inspection.......................................................................................................................................... 500
arp inspection-trust................................................................................................................................. 500
clear ip dhcp snooping............................................................................................................................... 501
clear ipv6 dhcp snooping binding........................................................................................................... 502
ip dhcp relay.......................................................................................................................................... 503
ip dhcp snooping...................................................................................................................................... 503
ipv6 dhcp snooping................................................................................................................................. 504
ipv6 dhcp snooping vlan......................................................................................................................... 505
ip dhcp snooping binding.......................................................................................................................... 505
IPv6 DHCP Snooping Binding................................................................................................................... 506
ip dhcp snooping database........................................................................................................507
ipv6 dhcp snooping database write-delay..............................................................................508
ip dhcp snooping database renew..........................................................................................508
ipv6 dhcp snooping database renew......................................................................................509
ip dhcp snooping trust............................................................................................................509
ipv6 dhcp snooping trust.........................................................................................................510
ip dhcp source-address-validation........................................................................................510
ip dhcp relay information-option............................................................................................511
ip dhcp snooping verify mac-address......................................................................................512
ipv6 dhcp snooping verify mac-address..................................................................................513
ip helper-address...................................................................................................................513
ipv6 helper-address.................................................................................................................514
show ip dhcp snooping............................................................................................................515
show ipv6 dhcp snooping.........................................................................................................517
Commands to Configure DNS .................................................................................................518
ip name-server.......................................................................................................................518
ip domain-name.....................................................................................................................519
ip domain-list........................................................................................................................519
ip host.....................................................................................................................................520
clear host................................................................................................................................521

14 Equal Cost Multi-Path (ECMP)..........................................................................................522
ecmp-group..............................................................................................................................522
hash-algorithm.......................................................................................................................523
hash-algorithm ecmp..............................................................................................................526
hash-algorithm seed................................................................................................................527
ip ecmp-group.........................................................................................................................528
ip ecmp weighted...................................................................................................................529
link-bundle-monitor enable.................................................................................................529
link-bundle-distribution trigger-threshold............................................................................530
show config...........................................................................................................................531
show link-bundle distribution...............................................................................................531

15 FIPS Cryptography.............................................................................................................533
fips mode enable.....................................................................................................................533
show fips status......................................................................................................................533
show ip ssh............................................................................................................................534
ssh.........................................................................................................................................535

16 Force10 Resilient Ring Protocol (FRRP)..........................................................................538
clear frrp................................................................................................................................538
debug frrp...............................................................................................................................539
description...............................................................................................................................540
disable.....................................................................................................................................541
interface...................................................................................................................................542
member-vlan............................................................................................................................543
mode.........................................................................................................................................544
7 GARP VLAN Registration (GVRP)........................................................................................................... 549
  clear gvrp statistics................................................................................................................................. 550
  debug gvrp.............................................................................................................................................. 551
  disable.................................................................................................................................................... 552
  garp timers.............................................................................................................................................. 553
  gvrp enable............................................................................................................................................. 554
  gvrp registration..................................................................................................................................... 555
  protocol gvrp.......................................................................................................................................... 556
  show config............................................................................................................................................ 556
  show garp timers..................................................................................................................................... 557
  show gvrp................................................................................................................................................ 558
  show gvrp statistics................................................................................................................................. 559

8 High Availability (HA)............................................................................................................................ 561
  patch flash://RUNTIME_PATCH_DIR........................................................................................................ 561
  process restartable................................................................................................................................... 562
  redundancy auto-failover-limit................................................................................................................ 563
  redundancy disable-auto-reboot............................................................................................................. 564
  redundancy force-failover....................................................................................................................... 565
  redundancy primary............................................................................................................................... 565
  redundancy protocol............................................................................................................................... 566
  redundancy reset-counter...................................................................................................................... 567
  redundancy sfm standby......................................................................................................................... 567
  redundancy synchronize......................................................................................................................... 569
  show patch............................................................................................................................................. 569
  show processes restartable..................................................................................................................... 570
  show redundancy.................................................................................................................................... 571

9 ICMP Message Types.............................................................................................................................. 574

10 Internet Group Management Protocol (IGMP).................................................................................... 576
  IGMP Commands..................................................................................................................................... 576
    clear ip igmp groups.............................................................................................................................. 576
    debug ip igmp....................................................................................................................................... 577
    ip igmp access-group........................................................................................................................... 578
    ip igmp immediate-leave....................................................................................................................... 579
    ip igmp last-member-query-interval.................................................................................................... 580
    ip igmp query-interval.......................................................................................................................... 581
    ip igmp query-max-resp-time................................................................................................................ 582
    ip igmp ssm-map.................................................................................................................................. 583
    ip igmp version.................................................................................................................................... 584
    show ip igmp groups............................................................................................................................. 585
    show ip igmp interface......................................................................................................................... 587
show ip igmp ssm-map................................................................. 589
IGMP Snooping Commands...................................................... 590
clear ip igmp snooping groups.............................................. 591
debug ip igmp snooping......................................................... 591
ip igmp snooping enable....................................................... 592
ip igmp snooping fast-leave.................................................. 593
ip igmp snooping flood......................................................... 594
ip igmp snooping last-member-query-interval..................... 595
ip igmp snooping mrouter..................................................... 596
ip igmp snooping querier...................................................... 597
show ip igmp snooping groups............................................. 598
show ip igmp snooping mrouter......................................... 599

21 Interfaces...........................................................................601
Basic Interface Commands.................................................. 601
clear counters..................................................................... 601
clear dampening................................................................. 603
dampening.......................................................................... 604
default interface.................................................................. 605
description......................................................................... 606
duplex (10/100 Interfaces)................................................... 607
flowcontrol......................................................................... 608
interface.............................................................................. 610
interface group................................................................... 612
interface loopback.............................................................. 613
interface managementEthernet......................................... 614
interface null....................................................................... 615
interface range.................................................................... 616
interface range macro (define)............................................ 618
interface range macro name............................................... 619
interface vlan...................................................................... 620
keepalive............................................................................ 621
negotiation auto................................................................. 622
monitor interface.................................................................. 624
mtu...................................................................................... 627
portmode hybrid.................................................................. 628
rate-interval......................................................................... 630
show config......................................................................... 631
show config (from INTERFACE RANGE mode)..................... 631
show interfaces..................................................................... 632
show interfaces configured............................................... 638
show interfaces dampening............................................... 639
show interfaces phy............................................................ 641
show interfaces stack-unit.................................................. 643
show interfaces status......................................................... 644
show interfaces switchport................................................ 646
show interfaces transceiver............................................... 647
show interfaces vlan.......................................................................................................................652
show range........................................................................................................................................653
show running-config ecmp-group...................................................................................................654
shutdown........................................................................................................................................655
speed (for 10/100/1000/10000 interfaces)....................................................................................656
speed (Management interface)..........................................................................................................657
switchport.........................................................................................................................................658
wavelength.......................................................................................................................................660
Egress Interface Selection (EIS) Commands.....................................................................................660
application.......................................................................................................................................660
application (for HTTP and ICMP)....................................................................................................661
clear management application pkt-cntr.........................................................................................662
clear management application pkt-fallback-cntr..........................................................................662
management egress-interface-selection..........................................................................................663
show ip management-eis-route........................................................................................................663
show management application pkt-cntr..........................................................................................664
show management application pkt-fallback-cntr........................................................................664
Port Channel Commands..................................................................................................................665
channel-member..............................................................................................................................665
group.................................................................................................................................................667
interface port-channel......................................................................................................................667
minimum-links.................................................................................................................................667
port-channel failover-group...............................................................................................................669
show config.....................................................................................................................................670
show interfaces port-channel..........................................................................................................671
show port-channel-flow....................................................................................................................674
Time Domain Reflectometer (TDR) Commands...............................................................................676
tdr-cable-test....................................................................................................................................676
show tdr............................................................................................................................................677
UDP Broadcast Commands...............................................................................................................678
debug ip udp-helper.........................................................................................................................678
ip udp-helper udp-port....................................................................................................................679
show ip udp-helper.........................................................................................................................680

22 Internet Protocol Security (IPSec)..............................................................................................681
crypto ipsec transform-set..............................................................................................................681
crypto ipsec policy............................................................................................................................683
management crypto-policy..............................................................................................................683
match.................................................................................................................................................684
session-key......................................................................................................................................685
show crypto ipsec transform-set.....................................................................................................686
show crypto ipsec policy....................................................................................................................687
transform-set..................................................................................................................................688

23 IPv4 Routing..................................................................................................................................689
arp.....................................................................................................................................................690
arp backoff-time..............................................................................................................................691
show ip traffic .............................................................................................................. 750
show tcp statistics ...................................................................................................... 753

### 24 IPv6 Access Control Lists (IPv6 ACLs) .............................................................. 755
- show cam-acl-egress ............................................................................................. 755
- show cam-acl .......................................................................................................... 756
- permit icmp ............................................................................................................ 758
- permit .................................................................................................................... 759
- ipv6 control-plane egress-filter ............................................................................. 760
- ipv6 access-list ...................................................................................................... 760
- cam-acl-egress ...................................................................................................... 761
- cam-acl .................................................................................................................. 763

### 25 IPv6 Basics ....................................................................................................... 765
- clear ipv6 fib .......................................................................................................... 765
- clear ipv6 route ...................................................................................................... 766
- clear ipv6 mld_host ............................................................................................... 767
- maximum dynamic-routes-ipv6 ............................................................................. 767
- ipv6 address autoconfig ....................................................................................... 768
- ipv6 address ......................................................................................................... 769
- ipv6 address eui64 ................................................................................................ 770
- ipv6 control-plane icmp error-rate-limit ............................................................. 771
- ipv6 flowlabel-zero .............................................................................................. 772
- ipv6 host ................................................................................................................ 772
- ipv6 name-server ................................................................................................. 773
- ipv6 nd dad attempts ............................................................................................ 774
- ipv6 nd dns-server ................................................................................................ 774
- ipv6 nd prefix ....................................................................................................... 775
- ipv6 route .............................................................................................................. 776
- ipv6 unicast-routing ............................................................................................. 778
- show ipv6 cam stack-unit ...................................................................................... 779
- show ipv6 control-plane icmp ............................................................................. 780
- show ipv6 fib stack-unit ....................................................................................... 781
- show ipv6 flowlabel-zero .................................................................................... 782
- show ipv6 interface ............................................................................................. 782
- show ipv6 mld_host ............................................................................................. 785
- show ipv6 route ................................................................................................... 786
- trust ipv6-diffserv ............................................................................................... 788

### 26 Intermediate System to Intermediate System (IS-IS) ...................................... 790
- adjacency-check ................................................................................................... 791
- advertise ............................................................................................................... 792
- area-password ...................................................................................................... 793
- clear config ......................................................................................................... 794
- clear isis .............................................................................................................. 795
- clns host ............................................................................................................... 795
- debug isis ............................................................................................................ 796
debug isis adj-packets.........................................................................................................................797
debug isis local-updates..........................................................................................................................798
debug isis snp-packets............................................................................................................................799
debug isis spf-triggers.............................................................................................................................800
debug isis update-packets.......................................................................................................................800
default-information originate..................................................................................................................801
description..................................................................................................................................................802
distance.....................................................................................................................................................803
distribute-list in.........................................................................................................................................804
distribute-list out.......................................................................................................................................805
distribute-list redistributed-ignore..........................................................................................................806
domain-password.......................................................................................................................................807
graceful-restart ietf....................................................................................................................................807
graceful-restart interval.............................................................................................................................808
graceful-restart restart-wait.....................................................................................................................809
graceful-restart t1......................................................................................................................................810
graceful-restart t2......................................................................................................................................810
graceful-restart t3......................................................................................................................................811
hello padding.............................................................................................................................................812
hostname dynamic.....................................................................................................................................813
ignore-lsp-errors.......................................................................................................................................814
ip router isis...............................................................................................................................................814
ipv6 router isis..........................................................................................................................................815
isis circuit-type..........................................................................................................................................816
isis csnp-interval......................................................................................................................................817
isis hello-interval.....................................................................................................................................818
isis hello-multiplier.................................................................................................................................819
isis hello padding.....................................................................................................................................819
isis ipv6 metric.........................................................................................................................................820
isis metric..................................................................................................................................................821
isis network point-to-point.......................................................................................................................822
isis password..........................................................................................................................................823
isis priority................................................................................................................................................824
is-type......................................................................................................................................................824
log-adjacency-changes.............................................................................................................................825
lsp-gen-interval.........................................................................................................................................826
lsp-mtu......................................................................................................................................................827
lsp-refresh-interval....................................................................................................................................828
max-area-addresses.................................................................................................................................829
max-lsp-lifetime.......................................................................................................................................829
maximum-paths........................................................................................................................................830
metric-style..............................................................................................................................................831
multi-topology..........................................................................................................................................832
net............................................................................................................................................................833
passive-interface......................................................................................................................................833
redistribute...............................................................................................................................................834
redistribute bgp.......................................................................................................................................836
redistribute ospf.......................................................................................................................... 837
router isis................................................................................................................................. 838
set-overload-bit......................................................................................................................... 839
show config............................................................................................................................. 840
show isis database..................................................................................................................... 841
show isis graceful-restart detail............................................................................................... 844
show isis hostname.................................................................................................................... 845
show isis interface...................................................................................................................... 846
show isis neighbors.................................................................................................................... 847
show isis protocol....................................................................................................................... 849
show isis traffic.......................................................................................................................... 850
spf-interval.................................................................................................................................. 851

27 Link Aggregation Control Protocol (LACP)...853
  clear lacp counters................................................................................................................... 853
debug lacp.................................................................................................................................... 854
lacp long-timeout......................................................................................................................... 855
lacp port-priority........................................................................................................................ 856
lacp system-priority..................................................................................................................... 857
port-channel-protocol lacp.......................................................................................................... 857
show lacp..................................................................................................................................... 858

28 Layer 2..................................................................................................................................... 860
MAC Addressing Commands....................................................................................................... 860
clear mac-address-table.............................................................................................................. 860
mac-address-table aging-time.................................................................................................... 861
mac-address-table disable-learning............................................................................................. 862
mac-address-table static............................................................................................................ 862
mac-address-table station-move refresh-arp............................................................................. 864
mac learning-limit....................................................................................................................... 864
mac learning-limit learn-limit-violation.................................................................................... 866
mac learning-limit mac-address-sticky..................................................................................... 867
mac learning-limit station-move-violation................................................................................ 868
mac learning-limit reset............................................................................................................. 869
show cam mac linecard (count)................................................................................................. 869
show cam mac linecard (dynamic or static).............................................................................. 870
show mac-address-table............................................................................................................ 872
show mac-address-table aging-time.......................................................................................... 874
show mac accounting destination............................................................................................. 875
show mac learning-limit............................................................................................................ 876

Virtual LAN (VLAN) Commands.............................................................................................. 877
default vlan-id............................................................................................................................ 877
default-vlan disable.................................................................................................................... 878
name........................................................................................................................................... 879
show config............................................................................................................................... 880
show vlan.................................................................................................................................... 881
tagged......................................................................................................................................... 884
track ip............................................................................................................... 885
untagged........................................................................................................... 886
Far-End Failure Detection (FEFD)...................................................................... 887
ddebug fefd........................................................................................................ 887
fe fd..................................................................................................................... 888
fe fd disable...................................................................................................... 889
fe fd interval...................................................................................................... 890
fe fd mode.......................................................................................................... 891
fe fd reset.......................................................................................................... 891
fe fd-global interval......................................................................................... 892
fe fd-global....................................................................................................... 893
show fe fd......................................................................................................... 894

29 Link Layer Discovery Protocol (LLDP)... ...................................................... 896

LLPD Commands............................................................................................ 896
advertise dot1-tlv............................................................................................ 896
advertise dot3-tlv............................................................................................ 897
advertise management-tlv.............................................................................. 898
advertise management-tlv (Interface)............................................................ 899
clear lldp counters.......................................................................................... 900
clear lldp neighbors......................................................................................... 901
ddebug lldp interface....................................................................................... 902
disable................................................................................................................ 903
hello.................................................................................................................. 904
management-interface.................................................................................... 904
mode.................................................................................................................. 905
multiplier........................................................................................................... 906
protocol lldp (Configuration).......................................................................... 907
protocol lldp (Interface).................................................................................. 907
show lldp neighbors......................................................................................... 908
show lldp statistics.......................................................................................... 909
show management-interface.......................................................................... 910
show running-config lldp................................................................................ 910

LLDP-MED Commands..................................................................................... 911
advertise med guest-voice............................................................................... 912
advertise med guest-voice-signaling............................................................... 913
advertise med location-identification............................................................ 914
advertise med power-via-mdi.......................................................................... 915
advertise med softphone-voice....................................................................... 916
advertise med streaming-video....................................................................... 917
advertise med video-conferencing................................................................. 918
advertise med video-signaling........................................................................ 919
advertise med voice......................................................................................... 920
advertise med voice-signaling....................................................................... 921

30 Microsoft Network Load Balancing............................................................. 922
mac-address-table static (for Multicast MAC Address)................................... 922
ip vlan-flooding.................................................................923

31 Multicast Source Discovery Protocol (MSDP).................................................924
  clear ip msdp peer........................................................................924
  clear ip msdp sa-cache................................................................925
  clear ip msdp statistic................................................................926
  debug ip msdp...........................................................................927
  ip msdp cache-rejected-sa...........................................................927
  ip msdp default-peer..................................................................928
  ip msdp log-adjacency-changes....................................................929
  ip msdp mesh-group..................................................................930
  ip msdp originator-id................................................................931
  ip msdp peer.............................................................................932
  ip msdp redistribute..................................................................933
  ip msdp sa-filter.......................................................................934
  ip msdp sa-limit.......................................................................935
  ip msdp shutdown....................................................................936
  ip multicast-msdp....................................................................936
  show ip msdp..........................................................................937
  show ip msdp sa-cache rejected-sa............................................938

32 Multiple Spanning Tree Protocol (MSTP).........................................................940
  debug spanning-tree mstp..........................................................940
  disable...................................................................................941
  forward-delay..........................................................................942
  hello-time...............................................................................943
  max-age..................................................................................944
  msti.......................................................................................945
  name.....................................................................................946
  protocol spanning-tree mstp.......................................................947
  revision..................................................................................948
  show config............................................................................949
  show spanning-tree mst configuration.......................................949
  show spanning-tree msti............................................................950
  spanning-tree.........................................................................953
  spanning-tree msti.................................................................953
  tc-flush-standard....................................................................955

33 Multicast................................................................................956
  IPv4 Multicast Commands..........................................................956
    clear ip mroute....................................................................956
    ip mroute............................................................................957
    ip multicast-limit...............................................................958
    ip multicast-routing...........................................................959
    show ip mroute.................................................................960
    show ip rpf.......................................................................962
34 Neighbor Discovery Protocol (NDP)............................................................................. 964
  clear ipv6 neighbors................................................................................................... 964
  ipv6 neighbor.............................................................................................................. 965
  show ipv6 neighbors................................................................................................... 967
  IPv6 Router Advertisement (RA) Guard................................................................. 968
    debug ipv6 nd ra-guard......................................................................................... 968
    device-role.............................................................................................................. 969
    hop-limit................................................................................................................. 969
    ipv6 nd ra-guard attach-policy........................................................................... 970
    ipv6 nd ra-guard enable....................................................................................... 971
    ipv6 nd ra-guard policy....................................................................................... 971
    managed-config-flag......................................................................................... 972
    match ra.............................................................................................................. 972
    mtu......................................................................................................................... 973
    other-config-flag............................................................................................... 974
    reachable-time..................................................................................................... 974
    retrans-time......................................................................................................... 975
    router-lifetime..................................................................................................... 975
    router-preference maximum............................................................................... 976
    show config......................................................................................................... 977
    show ipv6 nd ra-guard policy............................................................................. 978
    trusted-port......................................................................................................... 979

35 Object Tracking........................................................................................................ 980
  IPv4 Object Tracking Commands........................................................................... 980
    debug track.......................................................................................................... 980
    delay..................................................................................................................... 981
    description.......................................................................................................... 982
    show running-config track............................................................................... 983
    show track............................................................................................................ 984
    threshold metric.................................................................................................. 985
    track interface ip routing.................................................................................... 987
    track interface line-protocol.............................................................................. 988
    track ip host reachability................................................................................... 989
    track ip route metric threshold......................................................................... 989
    track ip route reachability................................................................................ 990
    track resolution ip route.................................................................................... 991
  IPv6 Object Tracking Commands........................................................................... 992
    show track ipv6 route........................................................................................ 992
    track interface ipv6 routing............................................................................... 993
    track ipv6 route metric threshold...................................................................... 994
    track ipv6 route reachability............................................................................. 995
    track resolution ipv6 route............................................................................... 996

36 Open Shortest Path First (OSPFv2 and OSPFv3).................................................... 999
  OSPFv2 Commands.................................................................................................. 999
<table>
<thead>
<tr>
<th><strong>Contents</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>area default-cost..........................................................999</td>
</tr>
<tr>
<td>area nssa............................................................................1000</td>
</tr>
<tr>
<td>area range.........................................................................1001</td>
</tr>
<tr>
<td>area stub...........................................................................1002</td>
</tr>
<tr>
<td>auto-cost............................................................................1003</td>
</tr>
<tr>
<td>clear ip ospf......................................................................1004</td>
</tr>
<tr>
<td>clear ip ospf statistics.........................................................1005</td>
</tr>
<tr>
<td>debug ip ospf......................................................................1006</td>
</tr>
<tr>
<td>default-information originate.................................................1008</td>
</tr>
<tr>
<td>default-metric.....................................................................1009</td>
</tr>
<tr>
<td>description.........................................................................1010</td>
</tr>
<tr>
<td>distance..............................................................................1011</td>
</tr>
<tr>
<td>distance ospf......................................................................1012</td>
</tr>
<tr>
<td>distribute-list in.................................................................1013</td>
</tr>
<tr>
<td>distribute-list out...............................................................1014</td>
</tr>
<tr>
<td>fast-convergence..................................................................1015</td>
</tr>
<tr>
<td>graceful-restart grace-period................................................1016</td>
</tr>
<tr>
<td>graceful-restart helper-reject.................................................1017</td>
</tr>
<tr>
<td>graceful-restart mode...........................................................1018</td>
</tr>
<tr>
<td>graceful-restart role...........................................................1019</td>
</tr>
<tr>
<td>ip ospf auth-change-wait-time.................................................1020</td>
</tr>
<tr>
<td>ip ospf authentication-key.......................................................1020</td>
</tr>
<tr>
<td>ip ospf cost..........................................................................1021</td>
</tr>
<tr>
<td>ip ospf dead-interval............................................................1022</td>
</tr>
<tr>
<td>ip ospf hello-interval............................................................1023</td>
</tr>
<tr>
<td>ip ospf message-digest-key......................................................1024</td>
</tr>
<tr>
<td>ip ospf mtu-ignore................................................................1025</td>
</tr>
<tr>
<td>ip ospf network...................................................................1026</td>
</tr>
<tr>
<td>ip ospf priority....................................................................1027</td>
</tr>
<tr>
<td>ip ospf retransmit-interval......................................................1028</td>
</tr>
<tr>
<td>ip ospf transmit-delay............................................................1029</td>
</tr>
<tr>
<td>log-adjacency-changes............................................................1029</td>
</tr>
<tr>
<td>maximum-paths.....................................................................1030</td>
</tr>
<tr>
<td>network area.......................................................................1031</td>
</tr>
<tr>
<td>passive-interface..................................................................1032</td>
</tr>
<tr>
<td>redistribute........................................................................1034</td>
</tr>
<tr>
<td>redistribute bgp..................................................................1035</td>
</tr>
<tr>
<td>redistribute isis..................................................................1036</td>
</tr>
<tr>
<td>router-id............................................................................1037</td>
</tr>
<tr>
<td>router ospf.........................................................................1038</td>
</tr>
<tr>
<td>show config......................................................................1039</td>
</tr>
<tr>
<td>show ip ospf......................................................................1040</td>
</tr>
<tr>
<td>show ip ospf asbr................................................................1042</td>
</tr>
<tr>
<td>show ip ospf database............................................................1043</td>
</tr>
<tr>
<td>show ip ospf database asbr-summary.......................................1044</td>
</tr>
<tr>
<td>show ip ospf database external...............................................1046</td>
</tr>
<tr>
<td>show ip ospf database network...............................................1049</td>
</tr>
</tbody>
</table>
show ip ospf database nssa-external.................................................................1051
show ip ospf database opaque-area................................................................1052
show ip ospf database opaque-as....................................................................1054
show ip ospf database opaque-link................................................................1055
show ip ospf database router...........................................................................1056
show ip ospf database summary.....................................................................1058
show ip ospf interface.....................................................................................1060
show ip ospf neighbor.....................................................................................1062
show ip ospf routes.........................................................................................1064
show ip ospf statistics.....................................................................................1065
show ip ospf timers rate-limit.........................................................................1068
show ip ospf topology......................................................................................1069
summary-address...........................................................................................1070
timers spf..........................................................................................................1071
timers throttle lsa all.......................................................................................1072
timers throttle lsa arrival..................................................................................1073

OSPFv3 Commands............................................................................................1074
area authentication..........................................................................................1074
area encryption...............................................................................................1075
auto-cost...........................................................................................................1077
clear ipv6 ospf process......................................................................................1078
debug ipv6 ospf bfd.........................................................................................1079
debug ipv6 ospf packet......................................................................................1080
default-information originate..........................................................................1081
graceful-restart grace-period...........................................................................1082
graceful-restart mode......................................................................................1083
ipv6 ospf area..................................................................................................1084
ipv6 ospf authentication...................................................................................1085
ipv6 ospf bfd all-neighbors..............................................................................1086
ipv6 ospf cost....................................................................................................1087
ipv6 ospf dead-interval....................................................................................1088
ipv6 ospf encryption.......................................................................................1089
ipv6 ospf graceful-restart helper-reject.........................................................1090
ipv6 ospf hello-interval...................................................................................1091
ipv6 ospf priority............................................................................................1092
ipv6 router ospf.............................................................................................1092
maximum-paths..............................................................................................1093
passive-interface.............................................................................................1094
redistribute.....................................................................................................1095
router-id..........................................................................................................1096
show crypto ipsec policy...................................................................................1097
show crypto ipsec sa ipv6.................................................................................1099
show ipv6 ospf database..................................................................................1101
show ipv6 ospf interface..................................................................................1103
show ipv6 ospf neighbor..................................................................................1104
timers spf........................................................................................................1105
37 Policy-based Routing (PBR)................................................................................................................................. 1107
  description....................................................................................................................................................................... 1107
  ip redirect-group............................................................................................................................................................ 1108
  ip redirect-list............................................................................................................................................................... 1109
  permit............................................................................................................................................................................... 1110
  redirect........................................................................................................................................................................... 1111
  seq................................................................................................................................................................................ 1113
  show cam pbr............................................................................................................................................................... 1115
  show ip redirect-list....................................................................................................................................................... 1116

38 PIM-Sparse Mode (PIM-SM)................................................................................................................................. 1117
  IPv4 PIM-Sparse Mode Commands............................................................................................................................. 1117
    clear ip pim rp-mapping........................................................................................................................................... 1117
    clear ip pim tib............................................................................................................................................................ 1118
    debug ip pim............................................................................................................................................................... 1119
    ip pim bsr-border....................................................................................................................................................... 1120
    ip pim bsr-candidate................................................................................................................................................ 1121
    ip pim dr-priority......................................................................................................................................................... 1122
    ip pim join-filter........................................................................................................................................................ 1122
    ip pim ingress-interface-map...................................................................................................................................... 1123
    ip pim neighbor-filter............................................................................................................................................... 1124
    ip pim query-interval................................................................................................................................................ 1125
    ip pim register-filter................................................................................................................................................ 1126
    ip pim rp-address....................................................................................................................................................... 1127
    ip pim rp-candidate.................................................................................................................................................... 1128
    ip pim sparse-mode.................................................................................................................................................... 1129
    ip pim sparse-mode sg-expiry-timer.......................................................................................................................... 1129
    ip pim ssm-range......................................................................................................................................................... 1130
    ip pim spt-threshold.................................................................................................................................................. 1132
    no ip pim snooping dr-flood........................................................................................................................................ 1132
    show ip pim bsr-router............................................................................................................................................... 1133
    show ip pim interface................................................................................................................................................. 1134
    show ip pim neighbor................................................................................................................................................ 1136
    show ip pim rp............................................................................................................................................................ 1137
    show ip pim snooping interface................................................................................................................................ 1138
    show ip pim snooping neighbor................................................................................................................................ 1139
    show ip pim snooping tib............................................................................................................................................ 1140
    show ip pim ssm-range............................................................................................................................................... 1142
    show ip pim summary............................................................................................................................................... 1143
    show ip pim tib............................................................................................................................................................ 1144
    show running-config pim........................................................................................................................................... 1146

39 Port Monitoring......................................................................................................................................................... 1147
  description....................................................................................................................................................................... 1147
  monitor multicast-queue................................................................................................................................................ 1148
  monitor session.............................................................................................................................................................. 1149
40 Private VLAN (PVLAN) .........................................................................................................................1156
  ip local-proxy-arp.................................................................................................................................1157
  private-vlan mode.................................................................................................................................1158
  private-vlan mapping secondary-vlan.................................................................................................1159
  switchport mode private-vlan...............................................................................................................1160

41 Per-VLAN Spanning Tree Plus (PVST+)... ...........................................................................................1162
  description............................................................................................................................................1162
  disable................................................................................................................................................1163
  extend system-id..................................................................................................................................1164
  protocol spanning-tree pvst................................................................................................................1165
  show spanning-tree pvst.....................................................................................................................1166
  spanning-tree pvst................................................................................................................................1169
  spanning-tree pvst err-disable...........................................................................................................1171
  tc-flush-standard................................................................................................................................1172
  vlan bridge-priority.............................................................................................................................1173
  vlan forward-delay.............................................................................................................................1174
  vlan hello-time....................................................................................................................................1175
  vlan max-age.......................................................................................................................................1176

42 Quality of Service (QoS)......................................................................................................................1177
  Global Configuration Commands...........................................................................................................1177
  qos-rate-adjust......................................................................................................................................1177
  Per-Port QoS Commands.......................................................................................................................1178
    dot1p-priority......................................................................................................................................1178
    rate police..........................................................................................................................................1179
    rate shape.........................................................................................................................................1180
    service-class dot1p-mapping..............................................................................................................1181
    service-class dynamic dot1p.............................................................................................................1182
    strict-priority queue.........................................................................................................................1183
  Policy-Based QoS Commands................................................................................................................1184
    bandwidth-percentage.......................................................................................................................1184
    class-map..........................................................................................................................................1185
    clear qos statistics............................................................................................................................1186
    description.........................................................................................................................................1187
    match ip access-group......................................................................................................................1188
    match ip dscp....................................................................................................................................1189
    match ip precedence........................................................................................................................1190
    match ip vlan....................................................................................................................................1192
    match ip vrf.......................................................................................................................................1192
    match mac access-group..................................................................................................................1193
Routing Information Protocol (RIP) .......................................................................................................................... 1231
  auto-summary......................................................................................................................................................... 1231
  clear ip rip........................................................................................................................................................... 1232
  debug ip rip........................................................................................................................................................... 1233
  default-information originate............................................................................................................................... 1234
  default-metric....................................................................................................................................................... 1235
  description............................................................................................................................................................. 1236
  distance................................................................................................................................................................... 1237
  distribute-list in..................................................................................................................................................... 1238
  distribute-list out.................................................................................................................................................... 1239

DSCP Color Map Commands........................................................................................................................................ 1226
  dscp........................................................................................................................................................................ 1226
  qos dscp-color-map.............................................................................................................................................. 1227
  qos dscp-color-policy.......................................................................................................................................... 1228
  show qos dscp-color-policy................................................................................................................................. 1229
  show qos dscp-color-map.................................................................................................................................. 1230

show qos class-map.................................................................................................................................................. 1209
show qos dot1p-queue-mapping.............................................................................................................................. 1210
show qos dot1p-queue-mapping.............................................................................................................................. 1210
show qos policy-map................................................................................................................................................ 1210
show qos policy-map-input...................................................................................................................................... 1212
show qos policy-map-output.................................................................................................................................. 1213
show qos qos-policy-input....................................................................................................................................... 1214
show qos qos-policy-output................................................................................................................................... 1215
show qos statistics.................................................................................................................................................. 1216
show qos wred-profile........................................................................................................................................... 1218
test cam-usage....................................................................................................................................................... 1219
threshold................................................................................................................................................................. 1220
trust........................................................................................................................................................................ 1222
wred......................................................................................................................................................................... 1223
wred ecn................................................................................................................................................................. 1224
wred-profile........................................................................................................................................................... 1225

match mac dot1p........................................................................................................................................................ 1194
match mac vlan......................................................................................................................................................... 1195
policy-aggregate....................................................................................................................................................... 1196
policy-map-input....................................................................................................................................................... 1197
policy-map-output................................................................................................................................................... 1198
qos-policy-input....................................................................................................................................................... 1199
qos-policy-output.................................................................................................................................................... 1200
queue egress............................................................................................................................................................ 1201
queue ingress........................................................................................................................................................... 1202
rate-police................................................................................................................................................................ 1203
rate-shape............................................................................................................................................................... 1204
service-policy input.................................................................................................................................................. 1205
service-policy output............................................................................................................................................... 1206
service-queue........................................................................................................................................................ 1207
set........................................................................................................................................................................... 1208
show qos dscp-color-policy................................................................................................................................. 1226
ip poison-reverse........................................................................................................1240
ip rip receive version................................................................................................1241
ip rip send version......................................................................................................1242
ip split-horizon..........................................................................................................1243
maximum-paths...........................................................................................................1244
neighbor......................................................................................................................1245
network........................................................................................................................1246
offset-list.......................................................................................................................1247
output-delay................................................................................................................1248
passive-interface..........................................................................................................1249
redistribute..................................................................................................................1250
redistribute isis.............................................................................................................1251
redistribute ospf...........................................................................................................1252
router rip.......................................................................................................................1253
show config...............................................................................................................1254
show ip rip database...................................................................................................1255
timer basic...................................................................................................................1256
version..........................................................................................................................1257

44 Remote Monitoring (RMON)......................................................................................1258
rmon alarm....................................................................................................................1259
rmon collection history...............................................................................................1260
rmon collection statistics............................................................................................1261
rmon event....................................................................................................................1262
rmon hc-alarm.............................................................................................................1263
show rmon...................................................................................................................1264
show rmon alarms......................................................................................................1265
show rmon events.......................................................................................................1266
show rmon hc-alarm....................................................................................................1267
show rmon history......................................................................................................1268
show rmon log.............................................................................................................1269
show rmon statistics.................................................................................................1270

45 Rapid Spanning Tree Protocol (RSTP).....................................................................1274
bridge-priority.............................................................................................................1274
debug spanning-tree rstp...........................................................................................1275
description..................................................................................................................1276
disable..........................................................................................................................1277
forward-delay.............................................................................................................1277
hello-time..................................................................................................................1278
max-age.......................................................................................................................1279
protocol spanning-tree rstp......................................................................................1280
show config.................................................................................................................1281
show spanning-tree rstp.............................................................................................1281
spanning-tree rstp......................................................................................................1283
tc-flush-standard.......................................................................................................1285
47 Security................................................................................................................................. 1288
AAA Accounting Commands .............................................................................................. 1288
  aaa accounting................................................................................................................. 1288
  accounting....................................................................................................................... 1290
  aaa accounting suppress................................................................................................. 1291
  aaa radius group............................................................................................................ 1291
  show accounting............................................................................................................ 1292
Authorization and Privilege Commands ............................................................................... 1293
  authorization.................................................................................................................... 1293
  aaa authorization commands......................................................................................... 1294
  aaa authorization config-commands.............................................................................. 1295
  aaa authorization exec.................................................................................................. 1296
  privilege level (CONFIGURATION mode)......................................................................... 1297
  privilege level (LINE mode).......................................................................................... 1298
Obscure Password Commands.............................................................................................. 1299
  service obscure-passwords............................................................................................. 1299
Authentication and Password Commands ............................................................................ 1300
  aaa authentication enable............................................................................................. 1300
  aaa authentication login................................................................................................ 1301
  access-class.................................................................................................................... 1303
  enable password............................................................................................................ 1304
  enable sha256-password............................................................................................... 1305
  enable restricted.............................................................................................................. 1305
  enable secret................................................................................................................... 1306
  login authentication........................................................................................................ 1308
  password........................................................................................................................ 1309
  password-attributes....................................................................................................... 1310
  service password-encryption......................................................................................... 1311
  show privilege................................................................................................................ 1312
  show users....................................................................................................................... 1313
  timeout login response.................................................................................................. 1314
  username........................................................................................................................ 1315
RADIUS Commands............................................................................................................ 1317
  debug radius.................................................................................................................... 1317
  ip radius source-interface.............................................................................................. 1317
  radius-server deadtime................................................................................................. 1318
  radius-server group....................................................................................................... 1319
  radius-server host.......................................................................................................... 1320
  radius-server vrf............................................................................................................. 1322
  radius-server key........................................................................................................... 1323
  radius-server retransmit................................................................................................. 1324
  radius-server timeout..................................................................................................... 1325
TACACS+ Commands........................................................................................................... 1326
  tacacs-server group....................................................................................................... 1326
debug tacacs+
ip tacacs source-interface

Port Authentication (802.1X) Commands:
dot1x authentication (Configuration)
dot1x authentication (Interface)
dot1x auth-fail-vlan
dot1x auth-server
dot1x guest-vlan
dot1x mac-auth-bypass
dot1x max-eap-req
dot1x port-control
dot1x quiet-period
dot1x reauthentication
dot1x reauth-max
dot1x server-timeout
dot1x supplicant-timeout
dot1x tx-period
show dot1x interface

SSH and SCP Commands:
crypto key generate
crypto key zeroize rsa
debug ip ssh
ip scp topdir
ip ssh authentication-retries
ip ssh cipher
ip ssh connection-rate-limit
ip ssh hostbased-authentication
ip ssh key-size
ip ssh mac
ip ssh password-authentication
ip ssh pub-key-file
ip ssh rekey
ip ssh rhostsfile
ip ssh rsa-authentication (Config)
ip ssh server
ip ssh server vrf
ip ssh source-interface
ip ssh vrf
show crypto
show ip ssh
show ip ssh client-pub-keys
show ip ssh rsa-authentication
ssh
Secure DHCP Commands........................................................................................................1369
  clear ip dhcp snooping.........................................................................................................1369
  ip dhcp relay.........................................................................................................................1370
  ip dhcp snooping..................................................................................................................1371
  ip dhcp snooping binding.......................................................................................................1371
  ip dhcp snooping database.....................................................................................................1372
  ip dhcp snooping database renew........................................................................................1373
  ip dhcp snooping trust............................................................................................................1374
  ip dhcp snooping source-address-validation........................................................................1374
  ip dhcp snooping vlan...........................................................................................................1375
  show ip dhcp snooping..........................................................................................................1375
Role-Based Access Control Commands.................................................................................1376
  aaa authorization role-only.................................................................................................1376
  enable..................................................................................................................................1377
  role......................................................................................................................................1378
  show role...............................................................................................................................1379
  show userroles.....................................................................................................................1380
  userrole.................................................................................................................................1381

48 Service Provider Bridging.................................................................................................1383
  debug protocol-tunnel..........................................................................................................1383
  protocol-tunnel....................................................................................................................1384
  protocol-tunnel destination-mac........................................................................................1385
  protocol-tunnel enable..........................................................................................................1386
  protocol-tunnel rate-limit....................................................................................................1387
  show protocol-tunnel...........................................................................................................1388

49 sFlow...............................................................................................................................1389
  sflow collector.....................................................................................................................1390
  sflow enable (Global)..........................................................................................................1391
  sflow ingress-enable.............................................................................................................1392
  sflow extended-switch enable............................................................................................1393
  sflow max-header-size extended........................................................................................1393
  sflow polling-interval (Global)..........................................................................................1394
  sflow polling-interval (Interface).......................................................................................1395
  sflow sample-rate (Global).................................................................................................1396
  sflow sample-rate (Interface)..............................................................................................1397
  show sflow..........................................................................................................................1398

50 Simple Network Management Protocol (SNMP) and Syslog.........................................1400
SNMP Commands................................................................................................................1400
  show snmp.............................................................................................................................1400
  show snmp engineID.............................................................................................................1401
  show snmp group..................................................................................................................1402
  show snmp user....................................................................................................................1403
  snmp ifmib ifalias long........................................................................................................1404
  snmp-server community.......................................................................................................1405
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)

Syslog Commands

clear logging
clear logging auditlog
default logging buffered
default logging console
default logging monitor
default logging trap
logging
logging buffered
logging console
logging extended
logging facility
logging history
logging history size
logging monitor
logging on
logging source-interface
logging synchronous
logging trap
logging version
show logging
show logging auditlog
show logging driverlog stack-unit
terminal monitor

51 SNMP Traps

52 Stacking
redundancy disable-auto-reboot
redundancy force-failover stack-unit
redundancy protocol
reset stack-unit
show redundancy
show system stack-ports
53 Storm Control............................................................................................................. 1462
  show storm-control broadcast................................................................................. 1463
  show storm-control multicast.................................................................................. 1463
  show storm-control unknown-unicast......................................................................... 1464
  storm-control broadcast (Configuration)................................................................. 1465
  storm-control broadcast (Interface)......................................................................... 1466
  storm-control multicast (Configuration)................................................................. 1467
  storm-control multicast (Interface)......................................................................... 1468
  storm-control PFC/LLFC......................................................................................... 1469
  storm-control unknown-unicast (Configuration)...................................................... 1469
  storm-control unknown-unicast (Interface).............................................................. 1470

54 Spanning Tree Protocol (STP)................................................................................ 1472
  bridge-priority........................................................................................................... 1472
  bpdu-destination-mac-address.................................................................................. 1473
  debug spanning-tree............................................................................................... 1474
  description................................................................................................................ 1475
  disable....................................................................................................................... 1475
  forward-delay........................................................................................................... 1476
  hello-time................................................................................................................ 1477
  max-age.................................................................................................................... 1478
  protocol spanning-tree............................................................................................ 1478
  show config.............................................................................................................. 1479
  show spanning-tree 0.............................................................................................. 1480
  spanning-tree.......................................................................................................... 1483

55 SupportAssist.......................................................................................................... 1486
  eula-consent............................................................................................................. 1486
  support-assist.......................................................................................................... 1488
  support-assist activate............................................................................................. 1488
  support-assist activity.............................................................................................. 1488
  SupportAssist Commands........................................................................................ 1489
    activity.................................................................................................................. 1489
    contact-company................................................................................................... 1490
    contact-person...................................................................................................... 1490
    enable.................................................................................................................... 1491
    server.................................................................................................................... 1491
  SupportAssist Activity Commands.......................................................................... 1492
    action-manifest get............................................................................................... 1492
    action-manifest install......................................................................................... 1493
    action-manifest remove....................................................................................... 1493
    action-manifest show........................................................................................... 1494
enable..................................................................................................................1494
SupportAssist Company Commands.................................................................1495
    address ........................................................................................................1495
    street-address ..........................................................................................1496
    territory ....................................................................................................1496
SupportAssist Person Commands ....................................................................1497
    email-address ............................................................................................1497
    phone ..........................................................................................................1497
    preferred-method .....................................................................................1498
    time-zone ..................................................................................................1499
SupportAssist Server Commands .....................................................................1499
    proxy-ip-address .......................................................................................1499
    enable ........................................................................................................1500
    url ................................................................................................................1501
    show eula-consent .....................................................................................1501
    show running-config ...............................................................................1502
    show support-assist status .....................................................................1503

56 System Time and Date ................................................................................1505
    clock summer-time date ........................................................................1505
    clock summer-time recurring .................................................................1507
    clock time zone ........................................................................................1508
    debug ntp ..................................................................................................1509
    ntp authenticate ......................................................................................1510
    ntp authentication-key ...........................................................................1511
    ntp broadcast client ................................................................................1512
    ntp disable ................................................................................................1512
    ntp multicast client ..................................................................................1513
    ntp master <stratum> .............................................................................1514
    ntp offset-threshold .................................................................................1514
    ntp server ..................................................................................................1515
    ntp source ..................................................................................................1516
    ntp trusted-key ..........................................................................................1517
    show clock ................................................................................................1518
    show ntp associations ...............................................................................1519
    show ntp vrf associations .......................................................................1520
    show ntp status ........................................................................................1521

57 Tunneling ....................................................................................................1523
    ip unnumbered ..........................................................................................1523
    ipv6 unnumbered .......................................................................................1524
    tunnel allow-remote .................................................................................1525
    tunnel destination ....................................................................................1526
    tunnel dscp ................................................................................................1526
    tunnel flow-label ......................................................................................1527
    tunnel hop-limit .......................................................................................1528
    tunnel keepalive .......................................................................................1528
tunnel-mode.................................................................................................................................1529
  tunnel source...............................................................................................................................1530

58 Uplink Failure Detection (UFD)...............................................................................................1532
  clear ufd-disable............................................................................................................................1532
  debug uplink-state-group................................................................................................................1533
  description........................................................................................................................................1534
  downstream.......................................................................................................................................1534
  downstream auto-recover..................................................................................................................1535
  downstream disable links..................................................................................................................1536
  enable..............................................................................................................................................1537
  show running-config uplink-state-group........................................................................................1537
  show uplink-state-group....................................................................................................................1538
  uplink-state-group...........................................................................................................................1539
  upstream.........................................................................................................................................1540

59 VLAN Stacking.............................................................................................................................1542
  dei honor.........................................................................................................................................1542
  dei mark...........................................................................................................................................1543
  member............................................................................................................................................1544
  stack-unit stack-group......................................................................................................................1545
  vlan-stack access............................................................................................................................1546
  vlan-stack compatible......................................................................................................................1546
  vlan-stack dot1p-mapping................................................................................................................1548
  vlan-stack protocol-type..................................................................................................................1548
  vlan-stack trunk...............................................................................................................................1549

60 Virtual Routing and Forwarding (VRF).....................................................................................1552
  ip vrf................................................................................................................................................1552
  ip http vrf........................................................................................................................................1553
  description.......................................................................................................................................1554
  ip vrf forwarding.............................................................................................................................1555
  ip route-export................................................................................................................................1556
  ip route-import................................................................................................................................1557
  ipv6 route-export..............................................................................................................................1558
  ipv6 route-import............................................................................................................................1558
  match source-protocol.....................................................................................................................1559
  redistribute......................................................................................................................................1560
  interface management......................................................................................................................1560
  maximum dynamic-routes...............................................................................................................1561
  show ip vrf.....................................................................................................................................1562
  show run vrf....................................................................................................................................1563

61 VLT Proxy Gateway......................................................................................................................1564
  proxy-gateway lldp..........................................................................................................................1564
  proxy-gateway static......................................................................................................................1565
  remote-mac-address exclude-vlan.................................................................................................1565
Virtual Link Trunking (VLT) .................................................................................................................. 1571
- back-up destination.............................................................................................................................. 1572
- clear vlt statistics................................................................................................................................. 1572
- delay-restore......................................................................................................................................... 1573
- delay-restore abort-threshold.............................................................................................................. 1574
- lacp ungroup member-independent..................................................................................................... 1575
- multicast peer-routing timeout............................................................................................................ 1576
- peer-link port-channel.......................................................................................................................... 1577
- peer-routing.......................................................................................................................................... 1577
- peer-routing-timeout.............................................................................................................................. 1578
- primary-priority.................................................................................................................................... 1579
- show vlt brief......................................................................................................................................... 1580
- show vlt backup-link............................................................................................................................... 1580
- show vlt counters................................................................................................................................... 1581
- show vlt detail......................................................................................................................................... 1583
- show vlt inconsistency............................................................................................................................. 1583
- show vlt mismatch.................................................................................................................................. 1584
- show vlt role.......................................................................................................................................... 1585
- show vlt statistics................................................................................................................................... 1586
- show vlt statistics igmp-snoop.............................................................................................................. 1588
- system-mac........................................................................................................................................... 1589
- unit-id.................................................................................................................................................... 1589
- vlt domain............................................................................................................................................ 1590
- vlt-peer-lag port-channel...................................................................................................................... 1591
- show vlt private-vlan.............................................................................................................................. 1591

Virtual Router Redundancy Protocol (VRRP) ......................................................................................... 1593
- IPv4 VRRP Commands............................................................................................................................ 1593
  - advertise-interval................................................................................................................................. 1593
  - authentication-type............................................................................................................................... 1594
  - clear counters vrrp............................................................................................................................... 1595
  - debug vrrp.......................................................................................................................................... 1596
  - description.......................................................................................................................................... 1597
  - disable................................................................................................................................................ 1598
  - hold-time.......................................................................................................................................... 1598
  - preempt.............................................................................................................................................. 1599
  - priority............................................................................................................................................. 1600
  - show config....................................................................................................................................... 1601
  - show vrrp.......................................................................................................................................... 1602
  - track.................................................................................................................................................. 1605
  - virtual-address............................................................................................................................... 1606
  - vrrp delay minimum......................................................................................................................... 1607
vrrp delay reload.................................................................................................................................1607
vrrp-group...........................................................................................................................................1608
version................................................................................................................................................1609
IPv6 VRRP Commands......................................................................................................................1610
clear counters vrrp ipv6.....................................................................................................................1610
debug vrrp ipv6..................................................................................................................................1611
show vrrp ipv6.......................................................................................................................................1612
vrrp-ipv6-group..................................................................................................................................1614
About this Guide

This guide provides information about the Dell Networking operating system (OS) command line interface (CLI). This book also includes information about the protocols and features supported in Dell Networking OS.

References

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

- Dell Networking OS Configuration Guide
- Dell Networking OS Installation Guide
- Dell Networking OS Quick Start Guide
- Dell Networking OS Release Notes

Topics:
- Objectives
- Audience
- Conventions
- Information Icons

Objectives

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

NOTE: For more information about when to use the CLI commands, see the Dell Networking OS Configuration Guide for your specific system.

Audience

The Dell Networking OS CLI Guide is intended for system administrators with an understanding of Layer 2 and Layer 3 networking technologies, who are responsible for configuring or maintaining networks.

Conventions

This guide uses the following conventions to describe command syntax:

- **Keyword**: Keywords are in Courier font and must be entered in the CLI as listed.
- **parameter**: Parameters are in italics and require a number or word to be entered in the CLI.
- **(X)**: Keywords and parameters within braces must be entered in the CLI.
- **[X]**: Keywords and parameters within brackets are optional.
- **x|y**: Keywords and parameters separated by a bar require you to choose one option.
Keywords and parameters separated by a double bar allow you to choose any or all of the options.

Information Icons

This guide uses the following information symbols:

- **NOTE:** The Note icon signals important operational information.
- **CAUTION:** The Caution icon signals information about situations that could result in equipment damage or loss of data.
- **WARNING:** The Warning icon signals information about hardware handling that could result in injury.
This chapter describes the command line interface (CLI) structure and command modes. The Dell Networking operating software commands are in a text-based interface that allows you to use the launch commands, change command modes, and configure interfaces and protocols.

Topics:
- Accessing the Command Line
- Multiple Configuration Users
- Obtaining Help
- Navigating the CLI
- Using the Keyword no Command
- Filtering show Commands
- Enabling Software Features on Devices Using a Command Option
- Command Modes

### Accessing the Command Line

Access the CLI through a serial console port or a Telnet session.

When the system successfully boots, enter the command line in EXEC mode.

#### NOTE:
You must have a password configured on a virtual terminal line before you can Telnet into the system. Therefore, you must use a console connection when connecting to the system for the first time.

**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:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>CLI Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell&gt;</td>
<td>EXEC</td>
</tr>
<tr>
<td>Dell#</td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>Dell(conf)#</td>
<td>CONFIGURATION</td>
</tr>
</tbody>
</table>

#### NOTE: For a list of all the command mode prompts, refer to the Command Modes section.

### Multiple Configuration Users

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

```
Dell#conf
% Warning: The following users are currently configuring the system:
```

[450x676]CLI Basics

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

Topics:
- Accessing the Command Line
- Multiple Configuration Users
- Obtaining Help
- Navigating the CLI
- Using the Keyword no Command
- Filtering show Commands
- Enabling Software Features on Devices Using a Command Option
- Command Modes

### Accessing the Command Line

Access the CLI through a serial console port or a Telnet session.

When the system successfully boots, enter the command line in EXEC mode.

#### NOTE:
You must have a password configured on a virtual terminal line before you can Telnet into the system. Therefore, you must use a console connection when connecting to the system for the first time.

**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:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>CLI Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell&gt;</td>
<td>EXEC</td>
</tr>
<tr>
<td>Dell#</td>
<td>EXEC Privilege</td>
</tr>
<tr>
<td>Dell(conf)#</td>
<td>CONFIGURATION</td>
</tr>
</tbody>
</table>

#### NOTE: For a list of all the command mode prompts, refer to the Command Modes section.

### Multiple Configuration Users

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

```
Dell#conf
% Warning: The following users are currently configuring the system:
```
When another user enters CONFIGURATION mode, Dell Networking OS sends a message similar to the following:

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

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

## Obtaining Help

As soon as you are in a Command mode, there are several ways to access help:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>at the prompt or after a keyword. There must always be a space before the ?.</td>
</tr>
<tr>
<td>help</td>
<td>at the prompt.</td>
</tr>
<tr>
<td>a keyword, and then enter a space and a ?.</td>
<td></td>
</tr>
<tr>
<td>a partial keyword, and then enter a ?.</td>
<td></td>
</tr>
</tbody>
</table>

The following is an example of entering `ip ?` at the prompt:

```
Dell(conf)#ip ?
access-list Named access-list
as-path BGP autonomous system path filter
community-list Add a community list entry
control-plane Control plane configuration
dhcp DHCP configuration commands
domain-list Domain name to complete unqualified host name
domain-lookup Enable IP Domain Name System hostname translation
domain-name Define the default domain name
ecmp Weighted Ecmp Configuration
ecmp-group ECMP Group Configuration
extcommunity-list Add a Extended community list entry
tp FTP configuration commands
helper-address DHCP relay agent configuration
host Add an entry to the ip hostname table
http HTTP configuration commands
icmp ICMP configuration commands
igmp Internet Group Management Protocol
max-frag-count Max. fragmented packets allowed in IP re-assembly
mroute Multicast routes and counters
msdp Multicast source discovery protocol
multicast-limit Max entries in Multicast TIB
multicast-msdp Enable IP multicast MSDP protocol
multicast-routing Enable IP multicast forwarding
name-server Specify addrss of name server to use
pim Protocol Independent Multicast
prefix-list Build a prefix list
radius Interface configuration for RADIUS
redirect-list Named redirect-list
route Establish static routes
route-export Export routes
route-import Import routes
```
When entering commands, you can take advantage of the following timesaving features:

- Commands are not case-sensitive.
- Enter partial (truncated) command keywords. For example, you can enter `int teng 1/1` for the `interface tengigabitethernet 1/1` command.
- Use the TAB key to complete keywords in commands.
- Use the up Arrow key to display the last enabled command.
- Use either the Backspace key or Delete key to erase the previous character.
- Use the left and right Arrow keys to navigate left or right in the Dell Networking OS command line.

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

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

## 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, see the command mode list in Accessing the Command Line.

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

**Using the Keyword no Command**

To disable, delete or return to default values, use the **no** form of the commands. For most commands, if you type the keyword *no* in front of the command, you disable that command or delete it from the running configuration. In this guide, the **no** form of the command is described in the Syntax portion of the command description.

**Filtering show Commands**

You can filter commands using the **show** command to find specific information, display certain information only, or begin the command output at the first instance of a regular expression or phrase.

Execute a **show** command and a pipe (|), and one of the following parameters and a regular expression to show output that either excludes or includes the specified parameters.

- **except** Displays only the text that does not match the pattern (or regular expression).
- **find** Searches for the first occurrence of a pattern.
- **grep** Displays text that matches a pattern.

The **grep** command option has an ignore-case suboption that makes the search case-insensitive. For example, the commands:

- `show run | grep Ethernet` Returns a search result with instances containing a capitalized Ethernet, such as interface TenGigabitEthernet 1/1.
- `show run | grep ethernet` Does not return the previous search result because it only searches for instances containing a noncapitalized ethernet.
- `show run | grep Ethernet ignore-case` Returns instances containing both Ethernet and ethernet.

- **no-more** Does not paginate the display output.
- **save** Copies the output to a file for future use.

**Displaying All Output**

Use the **no-more** option after the pipe to display all output at once — not one screen at a time. This operation is similar to **terminal length screen-length** except that the **no-more** option affects the output of just the specified command. For example: `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: `command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save.`

Enabling Software Features on Devices Using a Command Option

The capability to activate software applications or components on a device using a command is supported on this platform.

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

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

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

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

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

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

To display the state of Dell Networking OS features:

```
Dell# show feature
```

**Example of show feature output**

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

```
Feature     State
------------------------
VRF          Enabled
```

**feature vrf**

Enable the VRF application on a switch. Once enabled, you cannot deactivate the VRF application.

**Syntax**

```
feature vrf
```

**Defaults**

Disabled

**Command Modes**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, and S6000.</td>
</tr>
</tbody>
</table>

Activate the VRF application on a device using the feature vrf command in CONFIGURATION mode. The no feature vrf command is not supported on any platform.

show feature

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

Syntax: show feature

Command Modes: EXEC

EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, and S6000.</td>
</tr>
</tbody>
</table>

You can activate VRF application on a device by using the feature vrf command in CONFIGURATION mode. The no feature vrf command is not supported on any of the platforms.

Example:

Dell# show feature
Feature  State
---------  --------
VRF       Enabled
Dell#
Command Modes

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

BGP ADDRESS-FAMILY Mode

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

To enter BGP ADDRESS-FAMILY mode:

1. Verify that you are logged in to ROUTER BGP mode.
2. Enter the address-family command.
3. Enter the protocol type:
   - For IPv4, enter the ipv4 multicast command. The prompt changes to include conf-router_bgp_af for IPv4.

CLASS-MAP Mode

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

To enter CLASS-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the class-map command, and then enter the class map name. The prompt changes to include config-class-map.

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

CONFIGURATION Mode

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

To enter CONFIGURATION mode:

1. Verify that you are logged in to EXEC Privilege mode.
2. Enter the configure command. The prompt changes to include conf.

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

CONTROL-PLANE Mode

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

To enter CONTROL-PLANE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the control-plane-cpuqos command. The prompt changes to include conf-control-cpuqos.

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

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

To enter DHCP mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip dhcp server` command. The prompt changes to include `config-dhcp`.

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

DHCP POOL Mode

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

To enter DHCP POOL mode:
1. Verify that you are logged in to DHCP mode.
2. Enter the `pool` command then the pool name. The prompt changes to include `config-dhcp-pool-name`.

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

ECMP GROUP Mode

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

To enter ECMP GROUP mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ecmp-group` command then enter the ECMP group ID. The prompt changes to include `conf-ecmp-group-ecmp-group-id`.

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

EIS Mode

To enable or configure Egress Interface Selection (EIS), use EIS mode.

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

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

EXEC Mode

When you initially log in to the switch, by default, you are logged in to EXEC mode. This mode allows you to view settings and enter EXEC Privilege mode, which is used to configure the device.
When you are in EXEC mode, the > prompt is displayed following the host name prompt, which is “Dell” by default. You can change the host name prompt using the hostname command.

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

**EXEC Privilege Mode**

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

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

**EXTENDED COMMUNITY LIST Mode**

To enable and configure a BGP extended community, use EXTENDED COMMUNITY LIST mode.

To enter EXTENDED COMMUNITY LIST mode:

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

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

**FRRP Mode**

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

To enter FRRP mode:

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

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

**INTERFACE Mode**

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

To enter INTERFACE mode:

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

**NOTE:** In Dell Networking OS, the stack unit number and interfaces start from 0. But in Dell Networking OS Open Networking platforms, the stack unit number and interfaces start from 1.

The prompt changes to include the designated interface and slot/port number. For example:
### Prompt | Interface Type
--- | ---
Dell(conf-if)# | INTERFACE mode
Dell(conf-if-gi-1/1)# | Gigabit Ethernet interface then the slot/port information
Dell(conf-if-te-1/1)# | Ten-Gigabit Ethernet interface then slot/port information
Dell(conf-if-lo-0)# | Loopback interface number
Dell(conf-if-ru-0)# | Null Interface then zero
Dell(conf-if-po-0)# | Port-channel interface number The range is from 1 to 128.
Dell(conf-if-vl-0)# | VLAN Interface then VLAN number (range 1–4094)
Dell(conf-if-ma-1/1)# | Management Ethernet interface then slot/port information
Dell(conf-if-tu-0)# | Tunnel interface then tunnel ID.
Dell(conf-if-range)# | Designated interface range (used for bulk configuration).

---

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

To enter IP ACCESS LIST mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter either the `ip access-list standard` command or the `ip access-list extended` command. Include a name for the ACL. The prompt changes to include `conf-std-nacl` or `conf-ext-nacl`.

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

---

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

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

---

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

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

1. Enter the `protocol lldp` command. The prompt changes to include `conf-lldp` or `conf-if-interface-lldp`.

**LLDP MANAGEMENT INTERFACE Mode**

To enable and configure Link Layer Discovery Protocol (LLDP) on management interfaces, use LLDP MANAGEMENT INTERFACE mode.

To enter LLDP MANAGEMENT INTERFACE mode:

1. Verify that you are logged in to LLDP mode.
2. Enter the `management-interface` command. The prompt changes to include `conf-lldp-mgmtIf`.

**LINE Mode**

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

To enter LINE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `line` command. Include the keywords `console` or `vty` and their line number available on the switch. The prompt changes to include `config-line-console` or `config-line-vty`.

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

**MAC ACCESS LIST Mode**

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

To enter MAC ACCESS LIST mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the `mac access-list standard` command or the `mac access-list extended` command. Include a name for the ACL. The prompt changes to include `conf-std-macl` or `conf-ext-macl`.

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

**MONITOR SESSION Mode**

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

To enter MONITOR SESSION mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `monitor session` command, and then the session ID. The prompt changes to include `conf-mon-sess-sessionID`.

**MULTIPLE SPANNING TREE (MSTP) Mode**

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

To enter MULTIPLE SPANNING TREE mode:
OPENFLOW INSTANCE Mode

To enable and configure OpenFlow instances, use OPENFLOW INSTANCE mode.
To enter OPENFLOW INSTANCE mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `openflow of-instance` command, and then the OpenFlow ID number of the instance you want to create or configure. The prompt changes to include `conf-of-instance of-id`.

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

Per-VLAN SPANNING TREE (PVST+) Plus Mode

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

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

To enter PVST+ mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `protocol spanning-tree pvst` command. The prompt changes to include `conf-pvst`.

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

PORT-CHANNEL FAILOVER-GROUP Mode

To configure shared LAG state tracking, use PORT-CHANNEL FAILOVER-GROUP mode. For more information, see Port Channel Commands.
To enter PORT-CHANNEL FAILOVER-GROUP mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `port-channel failover-group` command. The prompt changes to include `conf-po-failover-grp`.

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

PREFIX-LIST Mode

To configure a prefix list, use PREFIX-LIST mode.
To enter PREFIX-LIST mode:
1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `ip prefix-list` command and the name for the prefix list. The prompt changes to include `conf-nprefixl`.

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

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

To enter PROTOCOL GVRP mode:

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

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

RAPID SPANNING TREE (RSTP) Mode

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

To enter RSTP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the protocol spanning-tree rstp command. The prompt changes to include conf-rstp.

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

ROUTE-MAP Mode

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

To enter ROUTE-MAP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the route-map map-name [permit | deny] [sequence-number] command. The prompt changes to include config-route-map.

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

ROUTER BGP Mode

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

To enter ROUTER BGP mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Use the router bgp command, and then enter the AS number. The prompt changes to include conf-router_bgp.

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

ROUTER ISIS Mode

To enable and configure Intermediate System to Intermediate System (ISIS), use ROUTER ISIS mode. For more information, see Intermediate System to Intermediate System (IS-IS).

To enter ROUTER ISIS mode:
1 Verify that you are logged in to CONFIGURATION mode.
2 Use the `router isis` command. The prompt changes to include `conf-router_isis`.

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

**ROUTER OSPF Mode**

To configure OSPF, use ROUTER OSPF mode. For more information, see [Open Shortest Path First (OSPFv2)](OpenShortestPathFirstOSPfv2).

To enter ROUTER OSPF mode:

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

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

**ROUTER OSPFV3 Mode**

To configure OSPF for IPv6, use ROUTER OSPFV3 mode.

To enter ROUTER OSPFV3 mode:

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

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

**ROUTER RIP Mode**

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

To enter ROUTER RIP mode:

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

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

**SPANNING TREE Mode**

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

To enter SPANNING TREE mode:

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

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

To enable and configure the SupportAssist, use SupportAssist mode. For more information, see SupportAssist.

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the support-assist command. The prompt changes to include conf-supportassist.

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

TRACE-LIST Mode

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

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

You can exit this mode by using the exit command.

VLT DOMAIN Mode

To enable and configure the VLT domain protocol, use VLT DOMAIN mode. For more information, see Virtual Link Trunking (VLT).
To enter VLT DOMAIN mode:

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

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

VRRP Mode

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

1. To enable VRRP globally, verify that you are logged in to CONFIGURATION mode.
2. Enter the vrrp-group command, and then enter the VRRP group ID. The prompt changes to include conf-if-interface-type-slot/port-vrid-vrrp-group-id.
This section contains command line interface (CLI) commands needed to manage the configuration files, as well as other file management commands.

Topics:
- boot system
- cd
- copy
- delete
- dir
- format
- fsck flash
- mkdir
- mount nfs
- rmdir
- upgrade system
- HTTP Copy via CLI
- rename
- restore factory-defaults
- show boot system
- show bootvar
- show file-systems
- show os-version
- show running-config
- show startup-config
- show version
- upgrade

**boot system**

Specify the location where the Dell Networking OS image used to boot the system is stored.

**Syntax**

```
boot system {gateway ip-address | stack-unit {stack-unit-number | all} {default | primary | secondary} {ftp: | nfsmount: | system: {A: | B: | bmp-boot} | tftp: | usbflash:})
```

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

**Parameters**

- `gateway` Enter the IP address of the default next-hop gateway for the management subnet.
- `ip-address` Enter an IP address in dotted decimal format.
- `stack-unit` Enter the stack-unit number for the master switch.
Enter the keyword **all** for all the stack units.

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

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

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Not configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>CONFIGURATION</td>
</tr>
</tbody>
</table>

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced the support for <strong>bmp-boot</strong> on the S-Series and Z-Series switches.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information

To display these changes in the show bootvar command output, save the running configuration to the startup configuration (using the copy command) and reload system.

Use the **bmp-boot** keyword only when the device boots up from bare metal provisioning (BMP). For an industrial standard upgraded device, the Dell networking OS stores the image partition upgraded from the DHCP offer in the **bmp-boot** option.
**cd**

Change to a different working directory.

**Syntax**

`cd [flash: | usbflash:] <directory name and path>`

**Parameters**

- **flash:** Use the keyword `flash:` to change the current directory to internal flash and its sub directories.
- **usbflash:** Use the keyword `usbflash:` to change the current directory to the inserted USB.
- **directory name and path** Enter the directory name and path as follows: `directory name ([[flash://]directory_path])`

**NOTE:** The `cd` command without any arguments will change the current directory to flash:

**Command Modes**

EXEC Privilege

**Command History**

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

**Version**

- 9.8(1.0) Introduced on the Z9100–ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Added NFS mount support. Introduced on the S6000-ON.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4810.
- 7.6.1.0 Introduced on the S-Series.
- 7.5.1.0 Introduced on the C-Series.
- E-Series Original command.

**copy**

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

**Syntax**

`copy source-file-url destination-file-url`

**Parameters**

- **compressed-config** Enter the keywords `compressed-config` to copy a file from the current system configuration.
- **flash:** Enter the keyword `flash:` to copy from the local file system `([[flash://]filepath])`.
- **ftp:** Enter the keyword `ftp:` to copy from the remote file system, IPv4, or IPv6, `([ftp://userid:password@hostip/filepath])`. 
http: Enter the keyword http: to copy from the remote file system, IPv4, or IPv6, (http: // hostip/filepath).
nfsmount: Enter the keyword nfsmount: to copy from the nfs mount file system (nfsmount:// <mount-point>/filepath).
running-config Enter the keywords running-config to copy from the current system configuration.
scp: Enter the keyword scp: to copy from the remote file system, IPv4, or IPv6, (scp:// userid:password@hostip/filepath).
startup-config Enter the keywords startup-config to copy from the startup configuration.
tftp: Enter the keyword tftp: to copy from the remote file system, IPv4, or IPv6, (tftp:// hostip/filepath).
usbflash: Enter the keyword usbflash: to copy the file to or from the external USB flash.

Command Modes EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON. Added the nfsmount:&lt;mount-point&gt; parameters that allow you to mount a remote NFS file system.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the compressed-config parameter.</td>
</tr>
<tr>
<td>9.3(0.1)</td>
<td>Added the http parameter on the S6000, Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added IPv6 addressing support for FTP, TFTP, and SCP.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added ushflash and rpm0usbflash commands on E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series and added the SSH port number to the SCP prompt sequence on all systems.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

Usage Information Dell Networking OS supports a maximum of 100 files at the root directory level on both the internal and external flash.

When copying a file to a remote location (for example, using Secure Copy [SCP]), enter only the keywords and Dell Networking OS prompts you for the rest of the information. For example, when using SCP, you can enter copy running-config scp: where running-config is the source and the target is specified in the ensuing prompts. Dell Networking OS prompts you to enter any required information for the named destination — remote destination, destination filename, user ID, password, and so forth.
When you use the `copy running-config startup-config` command to copy the running configuration (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, Dell Networking OS creates a backup file on the internal flash of the startup configuration.

Dell Networking OS supports copying the running-configuration to a TFTP server, an FTP server, or a remote NFS file system. For example:

- `copy running-config tftp:
- `copy running-config ftp:
- `copy running-config nfsmount://<mount-point>/filepath

You can compress the running configuration by grouping all the VLANs and the physical interfaces with the same property. You can store the operating configuration to the startup config in Compressed mode and perform an image downgrade without any configuration loss.

Example

```
Dell#copy running-config scp:
Address or name of remote host []: 192.168.1.1
Port number of the server [22]: 22
Destination file name [startup-config]:
User name to login remote host: username
Password to login remote host:
!
4080 bytes successfully copied
Dell#
```

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

Example

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

Example

```
Dell# copy scp: flash:
Address or name of remote host []: 10.11.199.134
Port number of the server [22]: 99
Source file name []: test.cfg
User name to login remote host: admin
Password to login remote host:
Destination file name [test.cfg]: test1.cfg
Dell#
```

Example

```
Dell# copy compressed-config compressed-cfg
!
6655 bytes successfully copied
Dell#
```

Example

```
Dell# copy compressed-config ftp:
Address or name of remote host []: 10.11.8.12
Destination file name [startup-config]:
User name to login remote host: spbalaji
Password to login remote host:
!
6655 bytes successfully copied
Dell#
```

Example

```
Dell# copy scp://admin:admin123@10.16.206.77/sample_file flash://sample_file
Dell#
```
Related Commands

- cd — changes the working directory.

**delete**

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

**Syntax**

```plaintext
delete {flash: | nfsmount: | usbflash:} [no-confirm]
```

**Parameters**

- `flash:` To delete a file or directory on the internal flash, enter `flash://` then the filename or directory name (`[flash://]filepath`).

- `nfsmount:` To delete a file or directory on the NFS-mounted file system, enter `nfsmount://` then the mount point and the file path (`nfsmount://filepath`).

  **NOTE:** While deleting a file directory on a remote NFS file system, you must specify the mount-point that indicates the working directory on the NFS file system. You cannot delete the root directory of the remote NFS file system.

- `usbflash:` To delete a file or directory on the external USB flash, enter `usbflash://` then the filename or directory name (`[usbflash://]filepath`).

- `no-confirm` (OPTIONAL) Enter the keywords no-confirm to specify that the Dell Networking OS does not require user input for each file prior to deletion.

**Command Modes**

EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.P5) | Introduced on the S4048-ON.
9.8(0.P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON. Added support for NFS mount.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
E-Series | Original command.
```markdown
**dir**

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

**Syntax**

```plaintext
dir [flash: | nfsmount: | usbflash:]
```

**Parameters**

- **flash:**
  
  For a directory on the internal Flash, enter `flash:// directory name`.

- **nfsmount:**
  
  For a file or directory on an NFS-mounted file system, enter `nfsmount:// then the mount point and file path`.

  **NOTE:** While displaying a file directory on a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot display details corresponding to the root directory of the remote NFS file system.

- **usbflash:**
  
  For a directory on the external USB flash, enter `usbflash:// directory name`.

**Command Modes**

- EXEC Privilege

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for NFS mount.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
Dell# dir
Directory of flash:

1 drwx 8192 Jan 01 1980 00:00:00 +00:00 .
2 drwx 3072 Dec 15 2014 06:27:10 +00:00 ..
3 drwx 4096 Jan 01 1980 00:02:44 +00:00 TRACE_LOG_DIR
4 drwx 4096 Jan 01 1980 00:02:44 +00:00 CORE_DUMP_DIR
5 d--- 4096 Jan 01 1980 00:02:44 +00:00 ADMIN_DIR
6 drwx 4096 Jan 01 1980 00:02:44 +00:00 RUNTIME_PATCH_DIR
7 drwx 4096 Nov 06 2014 06:57:06 +00:00 CONFIG_TEMPLATE
8 -rwx 4625 Nov 06 2014 06:55:28 +00:00 startup-config
9 drwx 4096 May 31 2013 02:49:46 +00:00 CONFD_LOG_DIR
```
Example (NFS Mount)

Dell# dir nfsmount:
Directory of nfsmount:
1 drwx 512 Jun 15 2015 02:47:57 +00:00 .
2 drwx 512 Jun 15 2015 02:47:57 +00:00 ..

nfsmount: 1463410688 bytes total (585719808 bytes free)

Dell#

Related Commands
- cd — changes the working directory.

format

Erase all existing files and reformat the file system. After the file system is formatted, files cannot be restored.

Syntax
format {flash: | usbflash:}

Defaults
None

Command Modes
EXEC Privilege

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series

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

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

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

Related Commands
- copy — copy the current configuration to either the startup-configuration file or the terminal.
- show file-systems — display information about the file systems on the system.
**fsck flash**

Checks the flash file system for errors.

**Syntax**

```
fsck {flash: | usbflash:}
```

**Parameters**

- **flash:**
  
  For a directory on the internal Flash, enter `flash://` directory name.

- **usbflash:**
  
  For a directory on the external USB flash, enter `usbflash://` directory name.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(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.
9.0.2.0 | Introduced on the S6000.
9.1(0.0) | Introduced on S4810 and Z9000.
8.3.19.0 | Introduced on S4820T.

**Usage Information**

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

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

**Related Commands**

- **copy** — copy one file to another location.
- **show file-systems** — display information about the file systems on the system.

**mkdir**

Creates a directory on the NFS mounted file system.

**Syntax**

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

**Command Modes**

CONFIGURATION
Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

- `rmdir` — remove a directory.

**mount nfs**

Mounts an NFS file system to a device.

**Syntax**

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

**Parameters**

Enter the following location keywords and information:

- `rhost:path` Enter the remote hosts’s path directory.
- `mount-point` Enter the folder name in the local file system.
- `username` (OPTIONAL) Enter the user name to access the device.
- `password` (OPTIONAL) Enter the password.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Example

Dell# mount nfs nfstest nfs-mount-point userid pwd
Dell#

Related Commands

- `cd` — change the working directory.
rmdir

Removes a directory from the NFS mounted file system.

Syntax

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

Command Modes

CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Example

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

Related Commands

- `mkdir` — create a directory.

upgrade system

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

Syntax

```
upgrade system {flash: | ftp: | nfsmount: | scp: | stack-unit stack-unit-id | stack-unit all} | tftp: | usbflash:} file-url {A: | B:}
```

Parameters

- `system` Enter the keyword `system` to upgrade the operating system (OS) image.
- `flash: file-url` Enter the keyword `flash:` and specify the location of the image file in the format `//directory-path` or press Enter to launch a prompt sequence.
- `ftp: file-url` Enter the keyword `ftp:` and specify the location of the image file in the format `//userid:password@host-ip/filepath` or press Enter to launch a prompt sequence.
- `nfsmount://<mount-point>/filepath` Enter the keyword `nfsmount:` and specify the location of the image file in the format `//<mount-point>/filepath`.
- `scp: file-url` Enter the keyword `scp:` and specify the location of the image file in the format `userid:password@host-ip/filepath` or press Enter to launch a prompt sequence.
- `stack-unit stack-unit-id` Enter the keyword `stack-unit` and specify the stack-unit ID to sync the image to that stack-unit.
- `stack-unit all` Enter the keyword `stack-unit` followed by the keyword `all` to sync the image on all stack-units.
**tftp: file-url**

Enter the keyword tftp: and specify the location of the image file in the format //host-ip/filepath or press Enter to launch a prompt sequence.

**usbflash: file-url**

Enter the keyword usbflash: and specify the location of the source file in the format //directory-path to upgrade from an external flash device or press Enter to launch a prompt sequence.

A: | B:

Specify the flash partition of the operating-system image to be upgraded.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

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

**Version** | **Description**
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Added support for NFS mount.
9.2(1.0) | Introduced on the Z9500.
9.0(0.0) | Added support for IPv6 for the file-url parameter.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000. Added support for the SSD on the Z9000 only.
8.3.7.0 | Introduced on the S4810.
7.7.1.0 | Added support for TFTP and SCP.
7.6.1.0 | Introduced on the S-Series.

**Usage Information**

RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [X:X:X:X::X]. For maximum flexibility this command accepts IPv6 host addresses with or without the square brackets.

After you upgrade the system image, by entering the command, specify the location where the Dell Networking OS image used to boot the system is stored (boot system), save the configuration to the start-up config file (write memory), and reload the system (reload).

**Example**

```
Dell# upgrade system tftp://10.11.8.12/dv-rainier-13 a:
Received block num: 50
Received block num: 64
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
..............................
93924044 bytes successfully copied
System image upgrade completed successfully.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image upgraded to all
Dell#
```
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

```
```

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

Parameters

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

Defaults None.

Command Modes EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3(0.1)</td>
<td>Introduced on the S6000, Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

Example

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

rename

Rename a file in the local file system.

Syntax

```
rename url url
```

Parameters

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

Command Modes EXEC Privilege

Command History

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

Restore factory defaults.

**Syntax**

```
restore factory-defaults stack-unit {stack-unit-number | all} {clear-all | bootvar | nvram}
```

**Parameters**

- `factory-defaults`: Return the system to its factory default mode.
- `stack-unit-number`: Enter the stack member unit identifier to restore only the mentioned stack-unit. The range is from 1 to 6.
- `all`: Enter the keyword `all` to restore all units in the stack.
- `bootvar`: Enter the keyword `bootvar` to reset boot line.
- `clear-all`: Enter the keywords `clear-all` to reset the NvRAM, boot environment variables, and the system startup configuration.
- `nvram`: Enter the keyword `nvram` to reset the NvRAM only.

**Command Modes**

EXEC Privilege

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Added bootvar as a new parameter.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.16.0 | Introduced on the MXL 10/40GbE Switch IO Module.

**Usage Information**

Restoring factory defaults deletes the existing startup configuration and all persistent settings (stacking, fan-out, 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.

Following are the factory-default environment variables:

- baudrate
- primary_boot
- secondary_boot
- default_boot
- ipaddr
- gatewayip
- netmask
- macaddr
- mgmtautoneg
- mgmtspeed100
- mgmtfullduplex

Each boot path variable (primary_boot, secondary_boot, and default_boot) is further split into the following three independent variables:

- primary_server, primary_file, and primary_type
- secondary_server, secondary_file, and secondary_type
- default_server, default_file, and default_type

⚠️ **NOTE:** For information on the default values that these variables take, refer to the Restoring Factory Default Environment Variables section in the Dell Networking OS Configuration guide.

**Example (all stack units)**

Dell# restore factory-defaults stack-unit all clear-all

* Warning - Restoring factory defaults will delete the existing startup-config and all persistent settings (stacking, fanout, etc.)*

* All the units in the stack will be split into standalone units.*

* After restoration the unit(s) will be powered-cycled immediately.*

* Proceed with caution!*  

Warning: Restore will delete the existing configuration and all persistent settings (stacking, fanout, etc.)

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

--- Restore status ---

Unit Nvram Config
---

1 Success Success
2 Success Success
3 Success Success
Power-cycling the unit(s).

Example (single stack)

Dell# restore factory-defaults stack-unit 1 clear-all
******************************************************
* Warning - Restoring factory defaults will delete the existing *
* startup-config and all 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 Success
Power-cycling the unit(s).
Dell#

Example (NvRAM all stack units)

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
------------------------
1 Success
2 Success
3 Success
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{stack-unit-id | all}

Parameters

all Enter the keyword all to display the boot image information for all stack units.
**show boot system stack-unit**

Enter the `stack-unit-id` to display boot image information for a stack-unit.

- **Defaults**
  - none

- **Command Modes**
  - EXEC
  - EXEC Privilege

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

  **Version** | **Description**
  --- | ---
  9.8(1.0) | Introduced on the Z9100-ON.
  9.8(0.0P5) | Introduced on the S4048-ON.
  9.8(0.0P2) | Introduced on the S3048-ON.
  9.7(0.0) | Introduced on the S6000-ON.
  9.2(1.0) | Introduced on the Z9500.
  9.0.2.0 | Introduced on the S6000.
  8.3.19.0 | Introduced on the S4820T.
  8.3.11.1 | Introduced on the Z9000.
  8.3.7.0 | Introduced on the S4810.
  7.7.1.0 | Introduced on the C-Series and E-Series.

**Example**

```
Dell# show boot system stack-unit 1
Current system image information in the system:
=============================================
  Type          Boot Type      A           B
  -----------------  ------------  -----------
Stack-unit 1  FLASH BOOT  9-0(2-1)  9-0[boot]
Dell#
```

---

**show bootvar**

Display the variable settings for the boot parameters.

- **Syntax**
  - `show bootvar`

- **Command Modes**
  - EXEC Privilege

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

  **Version** | **Description**
  --- | ---
  9.8(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.
**show file-systems**

Display information about the file systems on the system.

**Syntax**

```
show file-systems
```

**Command Modes**

EXEC Privilege

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Example**

Dell# show bootvar
PRIMARY IMAGE FILE =  system://B
SECONDARY IMAGE FILE =  tftp://10.16.127.35/Dell-SI-9-0-2-0.bin
DEFAULT IMAGE FILE =  system://A
LOCAL CONFIG FILE =  variable does not exist
PRIMARY HOST CONFIG FILE =  variable does not exist
SECONDARY HOST CONFIG FILE =  variable does not exist
PRIMARY NETWORK CONFIG FILE =  variable does not exist
SECONDARY NETWORK CONFIG FILE =  variable does not exist
CURRENT IMAGE FILE =  system://B
CURRENT CONFIG FILE 1 =  flash://startup-config
CURRENT CONFIG FILE 2 =  variable does not exist
CONFIG LOAD PREFERENCE =  local first
BOOT INTERFACE GATEWAY IP ADDRESS =  10.16.132.254
Reload Mode =  normal-reload
Dell#
### Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>size(b)</td>
<td>Lists the size (in bytes) of the storage location. If the location is remote, no size is listed.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Lists the available size (in bytes) of the storage location. If the location is remote, no size is listed.</td>
</tr>
<tr>
<td>Feature</td>
<td>Displays the formatted DOS version of the device.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of storage. If the location is remote, the word network is listed.</td>
</tr>
</tbody>
</table>
| Flags | Displays the access available to the storage location. The following letters indicate the level of access:  
  - r = read access  
  - w = write access |
| Prefixes | Displays the name of the storage location. |

### Related Commands

- `format flash` — erases all the existing files and reformats the file system in the internal flash memory.

### show os-version

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

**Syntax**

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

**Parameters**

- `file-url`  
  (OPTIONAL) Enter the following location keywords and information:  
  - For a file on the internal flash, enter flash:// followed by 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 USB port, enter usbflash://filepath.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

Example

Usage Information

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

**show running-config**

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

**Syntax**

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

**Parameters**

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

  - `aaa` for the current AAA configuration
  - `acl` for the current ACL configuration
  - `arp` for the current static ARP configuration
  - `as-path` for the current AS-path configuration
  - `bfd` for the current BFD configuration
  - `bgp` for the current BGP configuration
  - `boot` for the current boot configuration
  - `cam-profile` for the current CAM profile in the configuration
  - `class-map` for the current class-map configuration
  - `community-list` for the current community-list configuration

  NOTE: If you did not configure anything that entity, nothing displays and the prompt returns.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecmp-group</td>
<td>for the current ECMP group configuration</td>
</tr>
<tr>
<td>eis</td>
<td>for the current EIS configuration</td>
</tr>
<tr>
<td>ethernet</td>
<td>for the current Ethernet CFM configuration</td>
</tr>
<tr>
<td>fefd</td>
<td>for the current FEFD configuration</td>
</tr>
<tr>
<td>ftp</td>
<td>for the current FTP configuration</td>
</tr>
<tr>
<td>frrp</td>
<td>for the current FRRP configuration</td>
</tr>
<tr>
<td>fvrp</td>
<td>for the current FVRP configuration</td>
</tr>
<tr>
<td>gvrp</td>
<td>for the current GVRP configuration</td>
</tr>
<tr>
<td>host</td>
<td>for the current host configuration</td>
</tr>
<tr>
<td>hardware-monitor</td>
<td>for hardware-monitor action-on-error settings</td>
</tr>
<tr>
<td>hypervisor</td>
<td>for the current hypervisor configuration</td>
</tr>
<tr>
<td>igmp</td>
<td>for the current IGMP configuration</td>
</tr>
<tr>
<td>interface</td>
<td>for the current interface configuration</td>
</tr>
<tr>
<td>interface port-channel</td>
<td>for the current port-channel interface configuration.</td>
</tr>
<tr>
<td>interface tunnel</td>
<td>for all configured tunnels. For a specific tunnel, enter the tunnel ID. The range is from 1 to 16383.</td>
</tr>
<tr>
<td>ip</td>
<td>for the current IP configuration</td>
</tr>
<tr>
<td>isis</td>
<td>for the current ISIS configuration</td>
</tr>
<tr>
<td>line</td>
<td>for the current line configuration</td>
</tr>
<tr>
<td>lldp</td>
<td>for the current LLDP configuration</td>
</tr>
<tr>
<td>load-balance</td>
<td>for the current port-channel load-balance configuration</td>
</tr>
<tr>
<td>logging</td>
<td>for the current logging configuration</td>
</tr>
<tr>
<td>mac</td>
<td>for the current MAC ACL configuration</td>
</tr>
<tr>
<td>mac-address-table</td>
<td>for the current MAC configuration</td>
</tr>
<tr>
<td>management-eis</td>
<td>for the current management EIS configuration</td>
</tr>
<tr>
<td>management-route</td>
<td>for the current Management port forwarding configuration</td>
</tr>
<tr>
<td>mld</td>
<td>for the current MLD configuration</td>
</tr>
<tr>
<td>monitor</td>
<td>for the current Monitor configuration</td>
</tr>
<tr>
<td>mroute</td>
<td>for the current Mroutes configuration</td>
</tr>
<tr>
<td>msdp</td>
<td>for the current MSDP configuration</td>
</tr>
<tr>
<td>ntp</td>
<td>for the current NTP configuration</td>
</tr>
<tr>
<td>ospf</td>
<td>for the current OSPF configuration</td>
</tr>
<tr>
<td>pim</td>
<td>for the current PIM configuration</td>
</tr>
<tr>
<td>policy-map-input</td>
<td>for the current input policy map configuration</td>
</tr>
</tbody>
</table>
configured (OPTIONAL) Enter the keyword configuration to display line card interfaces with non-default configurations only.

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

compressed (Optional) Enter the keyword compressed to display the compressed group configuration. Displays the compressed configuration by grouping all similar configurations. The compression is done only for interface related configurations.
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

**Version** | **Description**
--- | ---
9.8(2.0) | Introduced on the S3100 series.
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.2.(0.0) | Added support for the tunnel and EIS interface types.
9.0.0.0 | Added support for the VLT option.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Added the hardware-monitor option.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
7.4.1.0 | Expanded to include the last configuration change, start-up last updated (date and time), and who made the change.
6.5.4.0 | Added the status option.

### Example

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

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

**show startup-config**

Display the startup configuration.

**Syntax**

`show startup-config`

**Command Modes**

- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on S-Series</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4(1.0)</td>
<td>Expanded to include the last configuration change, start-up last updated (date and time), and who made the change.</td>
</tr>
</tbody>
</table>

**Example**

Dell# show startup-config

```text
! Version 9-0(2-0)
! Last configuration change at Thu Apr 18 10:18:39 2013 by admin
! Startup-config last updated at Thu Apr 18 10:18:40 2013 by admin

boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.16.127.35/Dell-SI-9-0-2-0.bin
boot system stack-unit 0 default system: A:
boot system gateway 10.16.132.254

redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
... 
```

**Related Commands**

- `show running-config` — displays the current (running) configuration.
**show version**

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

**Syntax**

```
show version
```

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

**Command Fields**

- **Lines Beginning With**
  - Dell Networking...
  - Dell Operating...
  - Dell Application...
  - Copyright (c)...
  - Build Time...
  - Build Path...
  - Dell Networking OS uptime is...
  - System image...
  - System Type:
  - Control Processor...
  - 128K bytes...

- **Description**
  - Name of the operating system
  - OS version number
  - Software version
  - Copyright information
  - Software build’s date stamp
  - Location of the software build files loaded on the system
  - Amount of time the system has been up
  - Image file name
  - System name
  - Control processor information and amount of memory on processor
  - Amount and type of memory on system
upgrade

Upgrade the bootflash image or system image of the management unit.

Syntax

upgrade boot {all | bootflash-image | bootselector-image} stack-unit {stack-
unit-number | all} {booted | flash: | ftp: | nfsmount | scp: | tftp: |
usbflash:} file-url

Parameters

boot
Enter the keyword boot to change the boot image.

system
Enter the keyword system to change the system image.

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.

slot0:
After entering the keyword slot0:, 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.

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: flash://filepath or press Enter to launch a prompt sequence.

A: | B:
Enter the partition to upgrade from the flash.

stack-unit:
Enter the keywords stack-unit: to synch the image to the stack-unit.

file-url
Enter the following location keywords and information to upgrade using an Dell
Networking OS image other than the one currently running:

- To specify an Dell Networking OS image on the internal flash, enter flash://
  file-path/filepath.
- To specify an Dell Networking OS image on an FTP server, enter ftp://
  user:password@hostip/filepath.
- To specify an Dell Networking OS image on the external flash, enter slot0://
  file-path/filepath.
- To copy a file on a TFTP server, enter tftp://hostip/filepath/filepath.

where hostip is either an IPv4 dotted decimal address or an IPv6 URI [x::x::x] format
address.

Defaults
none
Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.0(0.0)</td>
<td>Added support for IPv6 for the file-url parameter.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000. Added support for the SSD on the Z9000 only.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added support for TFTP and SCP.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [X::X::X]. For maximum flexibility this command accepts IPv6 host addresses with or without the square brackets.

Reload Dell Networking OS after executing this command. To copy Dell Networking OS from the management unit to one or more stack members, use the upgrade system stack-unit (S-Series stack member) command.

Example

```
Dell# upgrade system?
ftp: Copy from remote file system (ftp://userid:password@hostip/filepath)
scp: Copy from remote file system (scp://userid:password@hostip/filepath)
tftp: Copy from remote file system (tftp://hostip/filepath)
Dell# upgrade system ftp://username:password@10.11.1.1/FTOS-SB-7.7.1.0.bin
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
...........................................................
12946259 bytes successfully copied
Dell# reload
Dell#
```
This section contains command information to configure and monitor the system, including Telnet, file transfer protocol (FTP), and trivial file transfer protocol (TFTP).

**banner exec**

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

**Syntax**

banner exec  

**Parameters**

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

**Defaults**

No banner is displayed.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original Command</td>
</tr>
</tbody>
</table>
Usage Information

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

Example

Dell(conf)# banner exec ?
LINE c banner-text c, where 'c' is a delimiting character
Dell(conf)# banner exec %
Enter TEXT message. End with the character '%'.
This is the banner
Dell(conf)# end
Dell# exit
2d18h1m: %STKUNIT1-M:CP %SEC-5-LOGOUT: Exec session is terminated on console

This is the banner
Dell con0 now available

Press RETURN to get started.
2d18h2m: %STKUNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful on console

This is the banner
Dell>

Related Commands

- `line` — enables and configures the console and virtual terminal lines to the system.

banner login

Set a message of the day banner to appear after 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).

Parameters

- `keyboard-interactive` Enter the keyboard-interactive keyword and then press Enter (carriage return) to retrieve the message banner prompt.
- `acknowledgement` Enter the acknowledgement keyword to require a positive acknowledgement from the user while logging in to the system.
- `c` Enter a delineator character to specify the start and end of the text banner. You cannot use the delineator character in the banner message.
- `line` Enter text string for your text banner message, with a maximum of 50 lines and up to 255 characters per line.

Defaults

No banner is configured and a carriage return (CR) is required when creating a banner.

Command Modes

- **CONFIGURATION**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced the <code>acknowledgement</code> keyword.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
Usage Information

Enter the banner login command, type one or more spaces and a delineator character, type the banner text, and then type the second delineator character. The message of the day banner displays first when you are connected to the router; otherwise the login banner and prompt appear. After you have logged in, the banner EXEC (if configured) displays.

Example

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

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

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

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

Related Commands

- `banner motd` — sets a Message of the Day banner.
- `banner exec` — enables the display of a text string when you enter EXEC mode.

banner motd

Set a message of the day (MOTD) banner.

Syntax

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

**Parameters**

- `c` Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).

- `line` Enter a text string for your MOTD banner the message with your delineator. The delineator is a percent character (%).

**Defaults**

No banner is configured.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.11.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Related Commands**

- `banner exec` — enables the display of a text string when you enter EXEC mode.
- `banner login` — sets a banner to display after successful login to the system.

---

**cam-acl**

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

**Syntax**

```plaintext
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos number l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos] number ecfmacl number {fcoeacl number} {iscsioptacl {0|2}} {openflow {4|8}}
```

**Parameters**

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

---

[Control and Monitoring](#)
Allocate space to each CAM region.

Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The ipv6acl range must be a factor of 2.

Enter 4 or 8 for the number of OpenFlow FP blocks.

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

Command Modes

CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Added support for the fcoe parameter on the S4810 and S4820T.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Added support for OpenFlow on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Added the keywords fcoeacl and iscsioptacl on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the keywords ecfmacl, vman-qos, and vman-dual-qos.</td>
</tr>
</tbody>
</table>
Usage Information

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

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks and these blocks cannot be reallocated. The ipv4acl profile range is from 1 to 4.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

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

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

cam-acl-vlan

Specify the number of VFP blocks allocated to OpenFlow.

Syntax

```
cam-acl-vlan {default | vlanopenflow {0|1}}
```

Defaults

Disabled.

Parameters

- **default**: Reset VLAN CAM ACL entries to default settings
- **vlanopenflow**: Enter the number 1 to allocate VFP blocks and enable OpenFlow.
  (Default) Enter the number 0 to disable OpenFlow.

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

Usage Information

Reboot the switch after changing the parameter values for changes to take effect.

For platform-specific instructions about using this command, see the SDN section of the Dell Networking OS Configuration Guide.
clear line

Reset a terminal line.

Syntax

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

Parameters

- **line-number**: Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
- **aux 0**: Enter the keywords aux 0 to reset the auxiliary port.
- **console 0**: Enter the keywords console 0 to reset the console port.
- **vty number**: Enter the keyword vty then a number to clear a terminal line. The range is from 0 to 9.

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

configure

Enter CONFIGURATION mode from EXEC Privilege mode.

Syntax

```
cfgure [terminal]
```
Parameters

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

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

Example

Dell# configure
Dell(conf)#

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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(9.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

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

- enable
- disable
- exit
- config

### Example

Dell(conf-if-gi-5/1)# do clear counters
Clear counters on all interfaces [confirm]
Dell(conf-if-gi-5/1)#
Dell(conf-if-gi-5/1)# do clear logging
Clear logging buffer [confirm]
Dell(conf-if-gi-5/1)#
Dell(conf-if-gi-5/1)# do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
Dell(conf-if-gi-5/1)#

### 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 Dell Networking OS. The range is from 0 to 15.

#### Defaults

15

#### Command Modes

EXEC

#### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
Version Description
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.0) Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
E-Series Original command.

Usage Information
Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the enable password command to configure a password for the enable command at a specific privilege level. If no privilege level is specified, the default is privilege level 15.

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

Related Commands
• enable password — configures a password for the enable command and to access a privilege level.

enable optic-info-update interval

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

Syntax

```
enable optical-info-update [interval seconds]
```

Parameters

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

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
Usage Information
To enable polling and to configure the polling frequency, use this command.

end

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

Syntax
end

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

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
### Version | Description
---|---
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series and E-Series.
E-Series | Original command.

### Related Commands
- `exit` — returns to the lower command mode.

---

**exec-timeout**

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

**Syntax**

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

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

**Parameters**

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

- **seconds**
  - (OPTIONAL) Enter the number of seconds. The range is from 0 to 2147483. The default is **0 seconds**.

**Defaults**

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

**Command Modes**

- **LINE**

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
**Description**

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

Example

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

**exit**

Return to the lower command mode.

**Syntax**

```
exit
```

**Command Modes**

- EXEC Privilege
- CONFIGURATION
- LINE, INTERFACE
- TRACE-LIST
- PROTOCOL GVRP
- SPANNING TREE
- MULTIPLE SPANNING TREE
- MAC ACCESS LIST
- ACCESS-LIST
- AS-PATH ACL
- COMMUNITY-LIST
- PREFIX-LIST
- ROUTER OSPF
- ROUTER RIP
- ROUTER ISIS
- ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
ftp-server enable

Enable FTP server functions on the system.

Syntax
ftp-server [vrf vrf-name] enable

Parameters
vrf vrf-name

Enter the keyword vrf and then the name of the VRF to enable the FTP server to listen to that VRF instance.

NOTE: Use this attribute to specify the VRF that is used by the FTP server to accept client connections. If no VRF is specified, then the default VRF is used.

Defaults
Disabled.

Command Modes
CONFIGURATION

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

Version Description
9.8(10) 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.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
E-Series Original command.

Example
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 Dell (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password: 
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size date time name
-------- ------ ------ --------
512 Jul-20-2004 18:15:00 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>

**ftp-server todir**

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

**Syntax**

```cmd
ftp-server todir directory
```

**Parameters**

- `directory` Enter the directory path.

**Defaults**

The internal flash is the default directory.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>
After you enable FTP server functions with the `ftp-server enable` command, Dell Networking recommends specifying a top-level directory path. Without a top-level directory path specified, the Dell Networking OS directs users to the flash directory when logging in to the FTP server.

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

## ftp-server username

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

**Syntax**
```
ftp-server username username password [encryption-type] password
```
To delete a user name and its password, use the `no ftp-server username username` command.

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

**Defaults**
Not enabled.

**Command Modes**
- CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>
hostname

Set the host name of the system.

Syntax

```
hostname name
```

Parameters

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

Defaults

```
Dell
```

Command Modes

```
CONFIGURATION
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series

Original command.

Usage Information

```
The hostname is used in the prompt.
```

ip http source-interface

Specify an interface as the source interface for HTTP connections.

Syntax

```
ip http source-interface interface
```

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

Parameters

- **interface**
  Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
• For a port channel interface, enter the keywords `port-channel` then a number.
• For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

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

Command Modes
CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.3(0.1)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Increased number of VLANs to 4094 (was 2094)</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Support added for S-Series</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series</td>
</tr>
</tbody>
</table>

**ip http vrf**

Configure an HTTP client with a VRF used to connect to the HTTP server.

**Syntax**

```
ip http vrf {management | vrf-name}
```

To undo the HTTP client configuration, use the `ip http vrf` command.

**Parameters**

- `management` Enter the keyword `management` for configuring the management VRF that uses an HTTP client.
- `vrf-name` Enter a VRF name that the HTTP client uses. If you do not specify a VRF name, the HTTP client uses the default VRF.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

To make the HTTP clients VRF-aware, use the `ip http vrf` command. The HTTP client uses the VRF name that you specify to reach the HTTP server. If you do not specify a VRF name, the HTTP client uses the default VRF.

**ip ftp password**

Specify a password for outgoing FTP connections.

**Syntax**

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

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

**Parameters**

- `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

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
Usage Information

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

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

Related Commands

`ip ftp source-interface`

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

**Syntax**

```
ip ftp source-interface  interface
```

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

**Parameters**

- `interface` - Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For a port-channel interface, enter the keywords port-channel then the port-channel ID.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.
  - For a tunnel interface, enter the keyword tunnel.

**Defaults**

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

**Command Modes**

- CONFIGURATION

**Command History**

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### ip ftp username

Assign a user name for outgoing FTP connection requests.

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

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

**Defaults**
No user name is configured.

**Command Modes**
- CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

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

**Related Commands**
- `ip ftp password` — sets the password for FTP connections.
**ip ftp vrf**

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

**Syntax**

```plaintext
ip ftp [vrf {vrf-name | management}]
```

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

**Parameters**

- **vrf-name**
  
Enter the `vrf-name` to specify the VRF that is used by the FTP client.

- **management**
  
Enter the keyword `management` to specify that the VRF used by the FTP client is a management VRF.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**ip telnet server enable**

Enable the Telnet server on the switch.

**Syntax**

```plaintext
ip telnet server enable
```

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

**Defaults**

Enabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to enable the Telnet server on the switch.
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ip ssh server` — enables the secure shell (SSH) server on the system.

## ip telnet server vrf

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

**Syntax**

```plaintext
ip telnet server vrf {vrf-name | any | management}
```

To undo the TELNET server configuration, use the `no ip telnet server [vrf vrf-name]` command.

**Parameters**

- `vrf-name` Enter the `vrf-name` to specify the VRF that is used by the TELNET server.
- `any` Enter the keyword `any` to enable server from any VRF.
- `management` Enter the keyword `management` to specify a management VRF that is used by the TELNET server.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>
Usage Information

You can enable the TELNET server on either a management VRF or a user-defined VRF but not both. If you do not specify a VRF name, then the TELNET server is enabled on the default VRF.

Example

Dell(conf)# ip telnet server vrf vrf1
Dell(conf)# no ip telnet server vrf
Dell(conf)# ip telnet server vrf management
Dell(conf)# no ip telnet server vrf
Dell(conf)#

`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
```

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

Parameters

- `interface`

Enter the following keywords and the interface information:

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

Defaults

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

Command Modes

CONFIGURATION

Command History

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(10)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5(1.0)</td>
<td>Added support for 4-port 40G line cards on ExaScale.</td>
</tr>
</tbody>
</table>
### ip telnet vrf

**Description**
Configures a TELNET client to use a specific VRF.

**Syntax**
```
ip telnet [vrf vrf-name]
```
To undo the TELNET client configuration, use the `ip telnet [vrf vrf-name]` command.

**Parameters**
- `vrf vrf-name`: Enter the keyword `vrf` and then the name of the VRF to specify the VRF that is used by the TELNET client.

**Defaults**
Disabled

**Command Modes**
- **CONFIGURATION**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**
If you configure a TELNET client to use a specific VRF, then you need not explicitly specify the same VRF during the TELNET client sessions corresponding to that VRF.

**Example**
```
Dell(conf)# ip telnet vrf vrf1
Dell(conf)# do telnet 10.10.10.2
Dell(conf)# no ip telnet vrf vrf1
Dell(conf)#
```
**ip tftp source-interface**

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

**Syntax**

```
ip tftp source-interface interface
```

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

**Parameters**

- `interface`
  
  Enter the following keywords and slot/port or number information:
  
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

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

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Increased number of VLANs to 4094 (was 2094).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command</td>
</tr>
</tbody>
</table>

**ip tftp vrf**

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

**Syntax**

```
ip tftp [vrf vrf-name]
```

Control and Monitoring | 109
To undo the TFTP client configuration, use the `no ip tftp [vrf vrf-name]` command.

**Parameters**

- **vrf vrf-name**
  
  Enter the keyword `vrf` and then the name of the VRF to specify the VRF that is used by the TFTP client.

**Defaults**

- Disabled

**Command Modes**

- CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

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

**Related Commands**

- `ftp-server topdir` — sets the directory to be used for incoming FTP connections.
- `ftp-server username` — sets a username and password for incoming FTP connections.

### line

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

**Syntax**

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

**Parameters**

- **aux 0**
  
  Enter the keyword `aux 0` to configure the auxiliary terminal connection.

- **console 0**
  
  Enter the keyword `console 0` to configure the console port. The console option is `<0-9>`.

- **vty number**
  
  Enter the keyword `vty` then a number from 0 to 9 to configure a virtual terminal line for remote sessions. The system supports 10 remote sessions.

- **end-number**
  
  (OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.

**Defaults**

- Not configured

**Command Modes**

- CONFIGURATION

**Command History**

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

Configures the limit of concurrent sessions for all users on console and virtual terminal lines.

**Syntax**

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

**Parameters**

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

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

**Defaults**

Not configured. You can use all the available sessions.

**Command Modes**

CONFIGURATION

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series**

Original command

### Description

You cannot delete a terminal connection.

### Related Commands

- `access-class` — restricts the incoming connections to a particular IP address in an IP access control list (ACL).
- `password` — specifies a password for users on terminal lines.
**Version**

9.8(0.0)

**Description**

Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.

### Usage Information

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

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

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

### Example

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

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

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

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

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

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

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

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

### Related Commands

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

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

Syntax

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

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables login statistics for the last 30 days by default.</td>
</tr>
<tr>
<td>time-period days</td>
<td>Sets the number of days the system stores user login statistics; range is from 1 to 30.</td>
</tr>
</tbody>
</table>

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.</td>
</tr>
</tbody>
</table>

Usage Information

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

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

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

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

Example

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

$ telnet 10.11.178.14
Trying 10.11.178.14...
Connected to 10.11.178.14.
Escape character is '^]'.
Login: admin
Password:
Last successful login: 12:52:01 UTC Tue Mar 22 2016 Line vty0 (10.11.178.14).
There were 1 unsuccessful login attempt(s) since the last successful login.
There were 1 unsuccessful login attempt(s) for user admin in the last 30 day(s).
There were 1 successful login attempt(s) for user admin in the last 30 day(s).
The preceding message shows that the user had previously logged in to the system using the VTY line from 10.11.178.14. It also displays the number of unsuccessful login attempts since the last login and the number of unsuccessful login attempts in the last 30 days.

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

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

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

**motd-banner**

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

**Syntax**

```
motd-banner
```

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

**Defaults**

Enabled on all lines.

**Command Modes**

- **LINE**

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series</td>
</tr>
</tbody>
</table>
ping

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

Syntax

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

Parameters

- **host**  
  (OPTIONAL) Enter the host name of the devices to which you are testing connectivity.

- **ip-address**  
  (OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.

- **ipv6-address**  
  (OPTIONAL) Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity.

- **count**  
  Enter the number of echo packets to be sent. The default is 5.
  - number: from 1 to 2147483647
  - continuous: transmit echo request continuously

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

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

- **source**  
  Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only. Enter the IP address in A.B.C.D format.
  - For a 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.
  - For a Tunnel interface, enter the keyword tunnel then a number from 1 to 16383.

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

- **df-bit**  
  (IPv4 only) Enter Y or N for the “don't fragment” bit in IPv4 header.
  - N: Do not set the "don't fragment" bit.
  - Y: Do set “don't fragment” bit
  Default is No.

- **validate-reply**  
  (IPv4 only) Enter Y or N for reply validation.
  - N: Do not validate reply data.
- Y: Do validate reply data.

Default is No.

**outgoing-interface**

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

**pattern**

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

**sweep-min-size**

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

**sweep-max-size**

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

**sweep-interval**

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

**interface**

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

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a 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.

**ethernet**

Enter the keyword ethernet to test layer2 connectivity.

**vrf vrf-name**

Enter the keyword vrf followed by the name of the VRF to test connectivity to the VRF.

**Defaults**

None.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0)P5</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)P2</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

Added support for the outgoing-interface option for link-local IPv6 addressing on the S4820T.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.12.0</td>
<td>Added support for the outgoing-interface option for link-local IPv6 addressing on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>IPv6 pinging available on management interface.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced extended ping options.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series (IPv6).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series (IPv4).</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for IPv6 address on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

When you enter the `ping` command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for Extended Commands.

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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point indicates receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period indicates the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench (destination too busy).</td>
</tr>
<tr>
<td>M</td>
<td>Could not fragment.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

**Example (IPv4)**

Dell# ping 172.31.1.255

Type Ctrl-C to abort.

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

**Example (IPv6)**

Dell# ping 100::1

Type Ctrl-C to abort.

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

Reboot the system.

**Syntax**

```
reload [conditional nvram-cfg-change | no-confirm [discard-running] | dell-diag
| onie [install | uninstall | rescue]]
```

**Parameters**

- `conditional nvram-cfg-change`  
  (OPTIONAL) Reload into the Dell Networking Operating System (OS) if the condition is true. A configuration change to the NVRAM requires a switch reload. To reload the switch, select `nvram-cfg-change`.

- `no-confirm [discard-running]`  
  Reload the chassis without prompting for further confirmation.

- `dell-diag`  
  (OPTIONAL) Reload the system into the Dell diagnostics mode.

- `onie`  
  (OPTIONAL) Reload the system into the ONIE mode. You can also use one of the following options to reload the system and enter the respective modes directly:
  - `install` — enter the Install mode and install the networking OS
  - `uninstall` — enter the Uninstall mode and uninstall the networking OS
  - `rescue` — enter the Rescue mode and access the file system

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Added the optional <code>dell-diag</code> and <code>onie</code> parameters. Introduced the <code>no-confirm</code> option.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Added ‘conditional’ parameter.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>
**Usage Information**

If you use only the `reload` command, the system boots into the Dell Networking OS.

If there is a change in the running configuration, the system prompts you to save the new configuration when you reload the system using the `reload` command. You can also save your running configuration manually using the `copy running-config` command.

You can use the `conditional` parameter if any configuration changes made to the NVRAM, such as, stack-group and fanout configurations, must be saved.

**Example**

The following example shows how to reload the system:

```bash
Dell# reload
Proceed with reload [confirm yes/no]: yes
```

The following example shows how to reload the system into Dell diagnostics mode:

```bash
Dell# reload dell-diag
Proceed with reload [confirm yes/no]: yes
```

The following example shows how to reload the system into ONIE mode:

```bash
Dell# reload onie
Proceed with reload [confirm yes/no]: yes
```

The following example shows how to reload the system into ONIE prompt and enter the install mode directly:

```bash
Dell# reload onie install
Proceed with reload [confirm yes/no]: yes
```

**send**

Send messages to one or all terminal line users.

**Syntax**

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

**Parameters**

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

**Defaults**

`none`

**Command Modes**

EXEC

**Command History**

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

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

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

### service timestamps

To debug and log messages, add time stamps. This command adds either the uptime or the current time and date.

**Syntax**

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

To disable timestamping, use the `no service timestamps {debug | log}` command.

**Parameters**

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

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
**Version** | **Description**
--- | ---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.0.0.0 | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.

**E-Series** | Original command.

**Usage Information**

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

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

---

**show alarms**

View alarms currently active in the system.

**Syntax**

```plaintext
show alarms [threshold]
```

**Parameters**

- **threshold** (OPTIONAL) Enter the keyword threshold to display the temperature thresholds in Celsius for each level.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.0.0.0 | Introduced on the Z9000.

### show alarms

Display the block sizes allocated for the VLAN CAM ACL.

**Syntax**

```plaintext
show cam-acl-vlan
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
Dell#show alarms
--  Minor Alarms  --
Alarm Type                                  Duration
-----------------------------------------------------------
--  Major Alarms  --
Alarm Type                                  Duration
-----------------------------------------------------------
PEM 2 in unit 1 down                        13 min, 36 sec
Fan 1 in PSU 2 of Unit 1 is down or removed 13 min, 34 sec
Dell#
```

### show cam-acl-vlan

Display the block sizes allocated for the VLAN CAM ACL.

**Syntax**

```plaintext
show cam-acl-vlan
```

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

### show command-history

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

**Syntax**

```plaintext
show command-history
```

**Defaults**

none

**Command Modes**

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

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

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

### Example

Dell# show command-history
[11/20 15:47:22]: CMD-(CLI):[service password-encryption]by default from console
- Repeated 3 times.
[11/20 15:47:23]: CMD-(CLI):[service timestamps log datetime]by default from console
[11/20 15:47:23]: CMD-(CLI):[enable password 7 *****]by default from console
[11/20 15:47:23]: CMD-(CLI):[username admin password 7 *****]by default from console
[11/20 15:47:23]: CMD-(CLI):[enable restricted 7 *****]by default from console
[11/20 15:47:23]: CMD-(CLI):[protocol spanning-tree rstp]by default from console
[11/20 15:47:23]: CMD-(CLI):[no disable]by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 1/1]by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 1.1.1.1 /24]by default from console
[11/20 15:47:23]: CMD-(CLI):[ip access-group abc in]by default from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown]by default from console
[11/20 15:47:23]: CMD-(CLI):[interface gigabitethernet 1/2]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from console
[11/20 15:47:23]: CMD-(CLI):[ip address 5.5.5.1 /24]by default from console
[11/20 15:47:23]: CMD-(CLI):[no shutdown]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from console
[11/20 15:47:23]: CMD-(CLI):[no ip address]by default from console
[11/20 15:47:23]: CMD-(CLI):[exit]by default from console
show cpu-traffic-stats

View the CPU traffic statistics.

Syntax

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

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.
- **cp**
  - (OPTIONAL) Enter the keyword cp to display traffic statistics on the specified CPU.

Defaults

```
all
```

Command Modes

```
EXEC
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

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 GigabitEthernet 8/2 Total packets:100
```
show debugging

View a list of all enabled debugging processes.

Syntax

show debugging

Command Modes

EXEC Privilege

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P6) 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(10) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
7.6.1.0 Introduced on the E-Series.
7.5.1.0 Introduced on the C-Series
E-Series Original command.

Example

Dell# show debug
Generic IP:
  IP packet debugging is on for
  ManagementEthernet 1/1
  Port-channel 1-2
  Port-channel 5
  GigabitEthernet 4/1-4/3,4/4-4/6,4/10-4/11,20
  GigabitEthernet 5/1-5/3,5/5-5/6,5/10-5/11,15,17,19,21
ICMP packet debugging is on for
**show environment**

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

**Syntax**

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

**Parameters**

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

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.0.0.0 | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.
7.8.1.0 | The output of the show environment fan command for the S Series is changed to display fan speeds instead of showing the fan status as up or down.

**Usage Information**

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

**Example (all)**

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

Speed in RPM
show inventory

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

**Syntax**

```
show inventory [media slot]
```

**Parameters**

- **media slot** (OPTIONAL) Enter the keyword `media` then the stack ID of the stack member for which you want to display pluggable media inventory.

  **NOTE:** This parameter is available but not supported in Dell Networking Operating System version 8.3.11.4. Because stacking is not supported, if you use this parameter, the output displays “Media not present or accessible” (refer to the Usage Information section).

**Defaults**

none

**Command Modes**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Output expanded to include Piece Part ID (PPID)</td>
</tr>
<tr>
<td></td>
<td>and eSR4 optics.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced this version of the command for S-</td>
</tr>
<tr>
<td></td>
<td>Series. S-Series output differs from E-Series.</td>
</tr>
</tbody>
</table>

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.

Related Commands
- show interfaces — displays the interface configuration.

show login statistics

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

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

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

Defaults
None

Command Modes
CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced the <code>successful-attempts</code> keyword.</td>
</tr>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.</td>
</tr>
</tbody>
</table>

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

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
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 all users on console and virtual terminal lines.
show memory

View current memory usage on the switch.

Syntax

```
show memory [stack-unit id]
```

Parameters

- `stack-unit id` (OPTIONAL) Enter the keyword `stack-unit` then the stack unit ID to display memory information on the designated stack member.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced this version of the command for the S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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

Example

```
Dell#show memory stack-unit 1
Statistics On Unit 1 Processor
===============================================
Total (b)    Used (b)      Free (b)       Lowest (b)       Largest (b)
3177185280   2310248       3174875032    3174676264   3174875032
Dell#
```

show processes cpu

Display CPU usage information based on processes running.

Syntax

```
```

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 sysdlp). Refer to Example (management-unit).

stack-unit id

(OPTIONAL) Enter the keyword stack-unit then the stack member ID.

As an option of the show processes cpu command, this option displays CPU usage for the designated stack member. Or, as an option of the command, 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 CPU utilization of processes related to stack-unit processing.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

Version          Description
9.8(0.0P5)       Introduced on the S4048-ON.
9.8(0.0P2)       Introduced on the S3048-ON.
9.7(0.0)         Introduced on the S6000-ON.
9.0.2.0          Introduced on the S6000.
9.0.0.0          Introduced on the Z9000.
8.3.19.0         Introduced on the S4820T.
8.3.11.1         Introduced on the Z9000.
8.3.7.0          Introduced on the S4810.
7.7.1.0          Added the keywords management-unit [details].
7.6.1.0          Introduced on the S-Series.

Example

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

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

Dell# show processes cpu stack-unit 1

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

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

PID        Runtime(ms)     Invoked       uSecs     5Sec    1Min     5Min TTY           Process
0xbb773000        5950         595       10000    1.00%   2.25%    1.22%   0          tExcTask
0xbab2a000        4030         403       10000    1.00%   1.33%    0.73%   0           frrpagt
0xbacf3000          10           1       10000    0.00%   0.00%    0.00%   0         F10StkMgr
0xbad0c000         710          71       10000    0.00%   0.00%    0.03%   0             lcMgr
0xbad24000          30           3       10000    0.00%   0.00%    0.00%   0               dla

132 | Control and Monitoring
show hardware stack-unit
show interfaces stack-unit
show hardware layer3

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

Related Commands
- show hardware layer2 acl — displays Layer 2 ACL data for the selected stack member and stack member port-pipe.
- show hardware layer3 — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.
- show hardware stack-unit — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.
- show hardware system-flow — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.
- show interfaces stack-unit — displays information on all interfaces on a specific S-Series stack member.
show processes memory (S-Series) — displays CPU usage information based on processes running in an S-Series.

show processes ipc flow-control

Display the single window protocol queue (SWPQ) statistics.

Syntax

show processes ipc flow-control [cp]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp</td>
<td>(OPTIONAL) Enter the keyword cp to view the control processor’s SWPQ statistics.</td>
</tr>
</tbody>
</table>

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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

Important Points:

- The SWP provides flow control-based reliable communication between the sending and receiving software tasks.
- A sending task enqueues messages into the SWP queue for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the SWP-2-NOMORETIMEOUT timeout message is generated.
- In the S-Series example, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example

```
Dell# show processes ipc flow-control cp
Q Statistics on CP Processor
TxProcess RxProcess Cur High Time Retr Msg Ack Aval Max
Len Mark Out ies Sent Rcvd Retra Retra
DHCP0 ACL0 0 1 1 1 1 1 25 25
DHCP0 IPMGR0 0 0 0 0 0 0 25 25
DHCP0 IPMGR1 0 0 0 0 0 0 25 25
DHCP0 IFMGR0 0 0 0 0 0 0 60 60
IPMGR0 NDPM0 0 0 0 0 0 0 60 60
IPMGR0 FEFD0 0 10 0 0 12 12 60 60
IPMGR0 SNMP0 0 1 0 0 1 1 60 60
IPMGR0 SFL CP0 0 20 0 0 26 26 60 60
IPMGR0 PORTMIRR0 0 8 0 0 9 9 60 60
IPMGR0 EVENTTERMLOG0 0 1 0 0 1 1 60 60
IPMGR0 IPSECMDR0 0 9 0 0 11 11 60 60
IPMGR0 DHCP0 0 8 0 0 11 11 60 60
IPMGR0 IFMGR0 0 29 0 0 36 36 60 60
IPMGR0 IFAGT3 0 1 0 0 2 2 60 60
IPMGR0 IFAGT3 0 1 0 0 1 1 60 60
IPMGR0 OSMDR0 0 16 1 1 21 21 60 60
IPMGR0 ACL0 0 8 0 0 14 14 60 60
IPMGR0 VRP0 0 10 0 0 17 17 60 60
IPMGR0 PIM0 0 1 0 0 1 1 5 5
IPMGR0 MACMDR0 0 0 0 0 0 0 60 60
IPMGR0 L2PM0 0 29 0 0 40 40 60 60
IPMGR0 DIFFSERVO 0 51 0 0 67 67 60 60
IPMGR0 RTM0 0 9 0 0 11 11 60 60
IPMGR0 LLDP0 0 12 0 0 12 12 60 60
IPMGR0 MSTM0 0 10 0 0 10 10 60 60
IPMGR0 IPMGR1 0 33 0 0 33 33 60 60
IPMGR0 LACP0 0 23 0 0 23 23 60 60
PORTMIRR0 ACL_AGENT2 0 0 0 0 0 50 50
IPMGR0 IGMP0 0 0 0 0 0 50 50
IPMGR0 IFAGT2 0 1 0 0 1 1 60 60
Dell#
```

**show processes memory**

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

**Syntax**

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

- **management-unit**: Enter the keyword `management-unit` for CPU memory usage of the stack management unit.
- **stack unit unit id**: Enter the keyword `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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S3048-ON and S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the <code>management-unit</code> option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total:</td>
<td>Total system memory available</td>
</tr>
<tr>
<td>MaxUsed:</td>
<td>Total maximum memory used ever (history indicated with time stamp)</td>
</tr>
<tr>
<td>CurrentUsed:</td>
<td>Total memory currently in use</td>
</tr>
<tr>
<td>CurrentFree:</td>
<td>Total system memory available</td>
</tr>
<tr>
<td>SharedUsed:</td>
<td>Total used shared memory</td>
</tr>
<tr>
<td>SharedFree:</td>
<td>Total free shared memory</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID</td>
</tr>
<tr>
<td>Process</td>
<td>Process Name</td>
</tr>
<tr>
<td>ResSize</td>
<td>Actual resident size of the process in memory</td>
</tr>
<tr>
<td>Size</td>
<td>Process test, stack, and data size</td>
</tr>
<tr>
<td>Allocs</td>
<td>Total dynamic memory allocated</td>
</tr>
</tbody>
</table>
show processes memory output

Field Description
Frees Total dynamic memory freed
Max Maximum dynamic memory allocated
Current Current dynamic memory in use

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

For the S-Series, the output of the show memory command and this command differ based on which Dell 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: 268435456, MaxUsed: 2420244, CurrentUsed: 2420244, CurrentFree: 266015212
TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
tme 435406 397536 54434 37870
ipc 16652 0 16652 16652
timerMgr 33304 0 33304 33304
sysAdmTsk 33216 0 33216 33216
tFib4 1943960 0 1943960 1943960
aclAgent 90770 16564 74206 74206
ifagt_1 21318 16564 21318 4754
dagt 6504 0 6504 6504
MacAgent 269778 0 269778 269778
Dell#

Example

Dell# show processes management-unit
CurrentUsed: 9848768, CurrentFree: 53088256
SharedUsed: 13007848, SharedFree: 7963696
PID Process ResSize Size Allocs Frees Max Current
337 KernLrnAgMv 117927936 0 0 0 0 0
331 vrrp 5189632 249856 50572 0 50572 50572
323 frpp 5206016 241664 369238 0 369238 369238
322 xstp 7430144 292864 38328 0 38328 38328
321 pm 5267456 823296 62168 0 62168 62168
314 igmp 4960256 380928 18588 18588 2024
313 mrtm 6742016 1130496 72758 0 72758 72758
309 l2mg 5607424 552960 735214 380972 619266 354242
301 l2pm 5001216 167936 1429522 1176044 286606 253478
298 arpm 4628480 217088 71092 33128 71092 37964
294 ospf 5468160 503808 62404 662560 78208 61644
288 dsm 6778880 1159168 39490 18588 39490 2024
287 rtm 5713920 602112 442280 198768 376024 243512
284 rip 4562944 258048 528 0 528 528
281 lacp 4673536 266240 221060 0 221060 221060
277 ipml 4837376 380928 83788 0 83788 83788
273 acl 5005312 512000 239564 149076 123616 90488
272 topoDPC 117927936 0 0 0 0 0
271 bcmNHOP 117927936 0 0 0 0 0
270 bcmDISC 117927936 0 0 0 0 0
269 bcmATP-RX 117927936 0 0 0 0 0
268 bcmATP-TX 117927936 0 0 0 0 0
267 bcmSPACK 117927936 0 0 0 0 0
266 bcmRX 117927936 0 0 0 0 0
265 bcmLINK.0 117927936 0 0 0 0 0
show software ifm

Display interface management (IFM) data.

Syntax

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

Parameters

- **clients**: Enter the keyword clients to display IFM client information.
- **summary**: (OPTIONAL) Enter the keyword summary to display brief information about IFM clients.
- **ifagt number**: Enter the keyword ifagt then the number of an interface agent to display software pipe and IPC statistics.
- **ifcb interface**: Enter the keyword ifcb then one of the following interface IDs then the interface information to display interface control block information for that interface:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- **stack-unit unit-ID**: Enter the keyword stack-unit then the stack member number to display IFM information for that unit.
- **trace-flags**: Enter the keyword trace-flags to display IFM information for internal trace flags.

Defaults

None.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S3048-ON and S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
</tbody>
</table>
show system

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

Syntax

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

Parameters

- `brief` (OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.
- `stack-unit unit-id` (OPTIONAL) Enter the keywords `stack-unit` then the stack member ID for information on that stack member.
- `stack-ports status` (OPTIONAL) Enter the keywords `stack-ports` for information about the status or topology of the stack ports.
- `topology` (OPTIONAL) Enter the keywords `topology` for information about the status or topology of the stack ports.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for the disabled-ports parameter.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
9.0.0.0 | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.4 | The brief parameter no longer displays the current Reload mode. To display Reload mode, use the show reload-type command. Modified the show system stack-unit command output to support Piece Part ID (PPID).
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | The Boot Flash field displays the code level for boot code 2.8.1.1 and newer, while older boot codes display as "Present".
7.7.1.0 | Added Master Priority field.
7.6.1.0 | Introduced on the S-Series.

Example (show system brief)

Dell# show system brief

```
Stack MAC                  : 34:17:eb:f2:90:c4
Reload-Type                : normal-reload [Next boot : normal-reload]
--  Stack Info  --
<table>
<thead>
<tr>
<th>Unit</th>
<th>UnitType</th>
<th>Status</th>
<th>ReqTyp</th>
<th>CurTyp</th>
<th>Version</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Member</td>
<td>not present</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Management</td>
<td>online</td>
<td>S4048-ON</td>
<td>S4048-ON</td>
<td>1-0(0-4160)</td>
<td>72</td>
</tr>
<tr>
<td>3</td>
<td>Member</td>
<td>not present</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Member</td>
<td>not present</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Member</td>
<td>not present</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Member</td>
<td>not present</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
--  Power Supplies  --
<table>
<thead>
<tr>
<th>Unit</th>
<th>Bay</th>
<th>Status</th>
<th>Type</th>
<th>FanStatus</th>
<th>FanSpeed(rpm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>up</td>
<td>AC</td>
<td>up</td>
<td>7048</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>down</td>
<td>UNKNOWN</td>
<td>down</td>
<td>0</td>
</tr>
</tbody>
</table>
--  Fan Status  --
<table>
<thead>
<tr>
<th>Unit</th>
<th>Bay</th>
<th>TrayStatus</th>
<th>Fan0</th>
<th>Speed</th>
<th>Fan1</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>up</td>
<td>up</td>
<td>7021</td>
<td>up</td>
<td>6971</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>up</td>
<td>up</td>
<td>7021</td>
<td>up</td>
<td>7072</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>up</td>
<td>up</td>
<td>6971</td>
<td>up</td>
<td>7021</td>
</tr>
</tbody>
</table>
```

Related Commands

- `show version` — displays the Dell Networking OS version.
- `show tech-support` — Display a collection of data from other show commands, necessary for Dell Networking technical support to perform troubleshooting.

**show tech-support**

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

**Syntax**

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

**Parameters**

- `stack-unit` (OPTIONAL) Enter the keywords stack-unit to view CPU memory usage for the stack member designated by unit-id.
- `page` (OPTIONAL) Enter the keyword page to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

When using the pipe command ( | ), enter one of these keywords to filter command output. For details about filtering commands, refer to CLI Basics.
**save**  
Enter the keyword `save` to save the command output.

`flash:` Save to local flash drive (flash://filename. A maximum of 20 characters.

**Command Modes**  
EXEC Privilege

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.P5) | Introduced on the S4048-ON
9.8(0.P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced `save` to the file options.
7.6.1.0 | Introduced on the S-Series.

**Usage Information**  
Without the `page` or `stack-unit` option, the command output is continuous. To interrupt the command output, use Ctrl-z.

The `save` option works with other filtering commands. This allows you to save specific information of a `show` command. The `save` entry must always be the last option. For example:  
```
Dell#show tech-support |grep regular-expression |except regular-expression | find regular-expression | save flash://result
```

This display output is an accumulation of the same information that is displayed when you execute one of the following `show` commands:

- `show version`
- `show clock`
- `show running-config`
- `show system stack-ports`
- `show interfaces`
- `show process memory`
- `show process cpu`
- `show file system`
- `show system`
- `show environment`
- `show ip traffic`
- `show ip management route`
- `show ip route summary`
- `show Inventory`
- `show log summary`
show command-history (last 20 commands)
show log

Example (S-Series)

Dell# show tech-support ?
page          Page through output
stack-unit    Unit Number
|             Pipe through a command
<cr>
Dell# show tech-support stack-unit 1 ?
|             Pipe through a command
<cr>
Dell# show tech-support stack-unit 1 | ?
except        Show only text that does not match a pattern
find          Search for the first occurrence of a pattern
grep          Show only text that matches a pattern
no-more        Don't paginate output
save          Save output to a file

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

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

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

Example

ssh-peer-stack-unit

Open an SSH connection to the peer stack-unit.

Syntax

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

Parameters

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

Defaults

Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
Connect through Telnet to a server. The Telnet client and server in Dell Networking support IPv4 and IPv6 connections. You can establish a Telnet session directly to the router or a connection can be initiated from the router.

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

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

### Parameters
- `host` Enter the name of a server.
- `ip-address` Enter the IPv4 address in dotted decimal format of the server.
- `ipv6-address prefix-length` Enter the IPv6 address in the `x:x:x:x::x` format then the prefix length in the `/x` format. The range is from `/0` to `/128`.
  
  **NOTE:** The `::` notation specifies successive hexadecimal fields of zeros.
- `vrf instance` (Optional) Enter the keyword `vrf` then the VRF instance name.
- `source-interface` (OPTIONAL) Enter the keywords `/source-interface` then the interface information to include the source interface. Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a Null interface, enter the keyword `null` then the Null interface number.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For Tunnel interface types, enter the keyword `tunnel` then the slot/port information. The range is from 1 to 16383.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

### Defaults
Not configured.

### Command Modes
- EXEC
- EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
Version | Description
------- | ----------------------------------
9.2(1.0) | Introduced on the Z9500.
9.0.2.0  | Introduced on the S6000.
9.0.0.0  | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810. Added support for source-interface for link-local IPv6 addressing.
8.3.11.1 | Introduced on the Z9000.
8.2.1.0  | Introduced on the E-Series (IPv6). Increased the number of VLANs to 4094 (was 2094).
8.1.1.0  | Introduced on the E-Series (IPv4).
7.6.1.0  | Introduced on the S-Series.
7.5.1.0  | Introduced on the C-Series and added support for IPv6 address on the E-Series only.

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

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

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

**Example**
```
Dell# telnet vrf vrf1 10.10.10.2
```

**telnet-peer-stack-unit**
Open a Telnet connection to the peer stack unit.

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

**Defaults**
Not configured.

**Command Modes**
- EXEC
- EXEC Privilege

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

**Version** | **Description**
------- | ----------------------------------
9.8(1.0)  | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0)  | Introduced on the S6000-ON.
### terminal length

Configure the number of lines displayed on the terminal screen.

**Syntax**

```
terminal length screen-length
```

**Parameters**

- `screen-length` Enter a number of lines. Entering zero causes the terminal to display without pausing. The range is from 0 to 512.

**Defaults**

24 lines

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
**traceroute**

View a packet’s path to a specific device.

**Syntax**

```
traceroute { host | vrf instance | ip-address | ipv6-address }
```

**Parameters**

- `host`
  - Enter the name of device.

- `vrf instance`
  - (Optional) E-Series Only: Enter the keyword `vrf` then the VRF Instance name.

- `ip-address`
  - Enter the IP address of the device in dotted decimal format.

- `ipv6-address`
  - Enter the IPv6 address, in the `x:x:x:x::x` format, to which you are testing connectivity.

**Defaults**

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

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series with IPv6.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series (IPv4 only).</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
7.4.1.0 | Added support for IPv6 address on the E-Series.
E-Series | Original command.

Usage Information
When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout (in seconds) (default is 5), a probe count (default is 3), minimum TTL (default is 1), maximum TTL (default is 30), and port number (default is 33434). To keep the default setting for those parameters, press the ENTER key.

For IPv6, you are prompted for a minimum hop count (default is 1) and a maximum hop count (default is 64).

Example (IPv4)
```
Dell# traceroute www.Dell Networking.com
Translating "www.Dell Networking.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.
-----------------------------------------------
Tracing the route to www.Dell Networking.com (10.11.84.18), 30 hops max, 40 byte packets
-----------------------------------------------
TTL Hostname      Probe1     Probe2     Probe3
1   10.11.199.190 001.000 ms 001.000 ms 002.000 ms
2   gwegress-sjc-02.Dell Networking.com (10.11.30.126) 005.000 ms 001.000 ms 001.000 ms
3   fw-sjc-01.Dell Networking.com (10.11.127.254) 000.000 ms 000.000 ms 000.000 ms
4   www.Dell Networking.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
Dell#
```

Example (IPv6)
```
Dell# traceroute 100::1
Type Ctrl-C to abort.
-----------------------------------------------
Tracing the route to 100::1, 64 hops max, 60 byte packets
-----------------------------------------------
Hops Hostname Probe1    Probe2    Probe3
1    100::1 000.000 ms 000.000 ms 000.000 ms
Dell#
```

Example (IPv6)
```
Dell# traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b
Type Ctrl-C to abort.
-----------------------------------------------
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b, 64 hops max, 60 byte packets
-----------------------------------------------
Hops Hostname Probe1    Probe2    Probe3
1    3ffe:501:ffff:100:201:e8ff:fe00:4c8b
  000.000 ms 000.000 ms 000.000 ms
Dell#
```

Related Commands
- `ping` — tests the connectivity to a device.

**undebug all**

Disable all debug operations on the system.

**Syntax**
```
undebug all
```
virtual-ip

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

Syntax

virtual-ip {ipv4-address | ipv6-address}  
To return to the default, use the no virtual-ip {ipv4-address | ipv6-address} command.

Parameters

- `ipv4-address` Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.).
- `ipv6-address` Enter an IPv6 address of the active management interface, in the x:x:x:x format.

Defaults

```
none
```

Command Modes

```
CONFIGURATION
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>
### Version | Description
--- | ---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.0.0.0 | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.5.1.0 | Introduced on the C-Series.
E-Series | Original command.

**Usage Information**

You can configure both IPv4 and IPv6 virtual addresses simultaneously, but only one of each. Each time this command is issued, it replaces the previously configured address of the same family, IPv4 or IPv6. The no virtual-ip command takes an address/prefix-length argument, so that the desired address only is removed. If you enter the no virtual-ip command without any specified address, then both IPv4 and IPv6 virtual addresses are removed.

**Related Commands**

- `ip address` — assigns a primary and secondary IP address to the interface.

### write

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

**Syntax**

```plaintext
write {memory compressed| 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.
- `compressed` : Enter the keyword `compressed` to write the operating configuration to the startup-config file in the compressed mode.
- `terminal` : Enter the keyword `terminal` to copy the current running configuration to the terminal. This command is similar to the show running-config command.

**Command Modes**

- EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `write memory` command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named “startup-configuration” (for example, you used a specific file during the `boot config` command), the running-config is not saved to that file; use the `copy` command to save any running-configuration changes to that local file.
802.1X

802.1X is a port-based Network Access Control (PNAC) that provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. Until the authentication, only extensible authentication protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking OS supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

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

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

Topics:

- debug dot1x
- dot1x auth-fail-vlan
- dot1x auth-server
- dot1x auth-type mab-only
- dot1x authentication (Configuration)
- dot1x authentication (Interface)
- dot1x critical-vlan
- dot1x guest-vlan
- dot1x host-mode
- dot1x mac-auth-bypass
- dot1x max-eap-req
- dot1x max-supplicants
- dot1x port-control
- dot1x profile
debug dot1x

Display 802.1X debugging information.

Syntax

```
debug dot1x [all | auth-pae-fsm | backend-fsm | eapol-pdu] [interface interface]
```

Parameters

- **all**: Enable all debugs in dot1x.
- **auth-pae-fsm**: Enable Authentication PAE FSM debugs in dot1x.
- **backend-fsm**: Enable Backend Auth FSM debugs in dot1x.
- **eapol-pdu**: Enable EAPOL frame trace in dot1x.
- **interface interface**: Restricts the debugging information to an interface. The interface option is available only when the interface is either operationally up or dot1x related interface configuration exists before enabling debugging for that interface.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>
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

- **vlan-id**: Enter the VLAN Identifier. The range is from 1 to 4094.
- **max-attempts number**: (OPTIONAL) Enter the keywords max-attempts followed number of attempts desired before authentication fails. The range is from 1 to 5. The default is 3.

Defaults

- **3 attempts**

Command Modes

- CONFIGURATION (conf-if-interface-slot/port)

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface moves to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next reauthentication interval (dot1x reauthentication).

Related Commands

- dot1x port-control — enable port control on an interface
- dot1x guest-vlan — configure a guest VLAN for limited access users or for devices that are not 802.1X capable.
- show dot1x interface — display the 802.1X configuration of an interface.
**dot1x auth-server**

Configure the authentication server to RADIUS.

**Syntax**

```
dot1x auth-server radius
```

**Defaults**
None

**Command Modes**
CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
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` — enable MAC authentication bypass.

---

**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

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Related Commands

- **dot1x authentication (Interface)** — enable dot1x on an interface.

**dot1x authentication (Interface)**

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

**Syntax**
```
[no] dot1x authentication
```

To disable dot1x on an interface, use the `no dot1x authentication` command.

**Defaults**
Disabled

**Command Modes**
INTERFACE

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- **dot1x authentication (Configuration)** — enable dot1x globally.

**dot1x critical-vlan**

Configure critical-VLAN for users or devices when authentication server is not reachable.

**Syntax**
```
[no] dot1x critical-vlan vlan-id
```

**Usage Information**

You can configure the VLAN that is generated on a VPC peer originated port when authentication fails on the VPC peer originated port.

**Example**

```
Switch(config-if)# dot1x critical-vlan 10
```
Enter the VLAN identifier. The VLAN-ID range is from 1 to 4094.

Not Configured.

INTERFACE

INTERFACE (BATCH MODE)

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9000 Series.</td>
</tr>
</tbody>
</table>

The dot1x critical-vlan command configures critical VLAN for the interface. If the authentication server is not reachable or not responding, the authenticator places the port or the supplicant in critical VLAN within the first attempt.

Use this command in Interface Batch mode to configure critical VLAN for users in a dual-homing setup.

Dell(conf)#show dot1x interface ten gigabit ethernet 0/41

802.1x information on Te 0/41:
-------------------------------------------
Dot1x Status:       Enable
Port Control:       AUTO
Port Auth Status:   AUTHORIZED (CRITICAL-VLAN)
Re-Authentication:  Enable
Untagged VLAN id:   400
     Guest VLAN: Enable
     Guest VLAN id: 400
     Auth-Fail VLAN: Enable
     Auth-Fail VLAN id: 400
     Auth-Fail Max-Attempts: 3
     Critical VLAN: Enable
     Critical VLAN id: 400
     Mac-Auth-Bypass: Disable
     Mac-Auth-Bypass Only: Disable
     Tx Period: 30 seconds
     Quiet Period: 60 seconds
     ReAuth Max: 2
     Supplicant Timeout: 30 seconds
     Server Timeout: 30 seconds
     Re-Auth Interval: 60 seconds
     Max-EAP-Req: 2
     Host Mode: SINGLE_HOST
     Auth PAE State: Authenticated
     Backend State: Idle
**dot1x guest-vlan**

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

**Syntax**

`dot1x guest-vlan vlan-id`

To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

**Parameters**

- **vlan-id**: Enter the VLAN Identifier. The range is from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION (conf-if-interface-slot/port)

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series, E-Series, and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication, for the device, occurs at the next reauthentication interval (dot1x reauthentication).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (dot1x auth-fail-vlan).

**NOTE:** You can create the Layer 3 portion of a guest VLAN and authentication fail VLANs regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

**Related Commands**

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

**dot1x host-mode**  
Enable single-host or multi-host authentication.

**Syntax**  
dot1x host-mode {single-host | multi-host | multi-auth}

**Parameters**
- **single-host**  
  Enable single-host authentication.
- **multi-host**  
  Enable multi-host authentication.
- **multi-auth**  
  Enable multi-suppliant authentication.

**Defaults**  
single-host

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added the multi-auth option on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>Added the single-host and multi-host options on the C-Series, E-Series, and S-Series.</td>
</tr>
</tbody>
</table>

**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-suppliant mode authenticates every device attempting to connect to the network on the authenticator port.

**Related Commands**
- `show dot1x interface` — display the 802.1X configuration of an interface.
**dot1x mac-auth-bypass**

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

**Syntax**

```
dot1x mac-auth-bypass
```

To disable MAC authentication bypass on a port, use the `no dot1x mac-auth-bypass` command.

**Defaults**

Disabled

**Command Modes**

INTERFACE

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To disable MAC authentication bypass on a port, enter the `no dot1x mac-auth-bypass` command.

**dot1x max-eap-req**

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

**Syntax**

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

**Parameters**

- `number`:
  
  Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is 2.

**Defaults**

2

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
dot1x max-supplicants

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in Multi-auth mode.

Syntax

    dot1x max-supplicants number

Parameters

    number  Enter the number of supplicants that can be authenticated on a single port in Multi-auth mode. The range is from 1 to 128. The default is 128.

Defaults

    128 hosts can be authenticated on a single authenticator port.

Command Modes

    INTERFACE

Command History

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

Version     Description

9.8(1.0)     Introduced on the Z9100–ON.
9.8(0.0P5)   Introduced on the S4048-ON.
9.8(0.0P2)   Introduced on the S3048-ON.
9.7(0.0)     Introduced on the S6000–ON.
9.2(1.0)     Introduced on the Z9500.
9.0.2.0      Introduced on the S6000.
9.0.0.0     Introduced on the Z9000.
8.3.19.0     Introduced on the S4820T.
8.3.12.0     Introduced on the S4810.
8.3.11.1     Introduced on the Z9000.
7.6.1.0      Introduced on the C-Series and S-Series.
7.4.1.0      Introduced on the E-Series.
dot1x port-control

Enable port control on an interface.

Syntax

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

Parameters

- **force-authorized**: Enter the keywords force-authorized to forcibly authorize a port.
- **auto**: Enter the keyword auto to authorize a port based on the 802.1X operation result.
- **force-unauthorized**: Enter the keywords force-unauthorized to forcibly de-authorize a port.

Defaults

None

Command Modes

Auto

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
7.6.1.0 Introduced on the C-Series and S-Series.
7.4.1.0 Introduced on the E-Series.

Usage Information

The authenticator completes authentication only when you set port-control to auto.

dot1x profile

Configure a dot1x profile to define a list of trusted supplicant MAC addresses.

Syntax

[no] dot1x profile profile-name
Parameters

profile-name

Enter a dot1x profile-name. The profile name length is limited to 32 characters.

Defaults

None

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Error Strings

NONE

Command History

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010.</td>
</tr>
</tbody>
</table>

Usage Information

The dot1x profile command configures a dot1x profile to define a list of trusted supplicant MAC addresses. Maximum number of dot1x profiles is limited to 10. This command launches dot1x profile mode for entering profile related commands such as the mac command. The dot1x static-mab command assigns the dot1x profile to an interface.

Use this command in Configuration Terminal Batch mode to configure the dot1x profile in a dual-homing setup.

Related Commands

- dot1x static-mab
- mac

**dot1x quiet-period**

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

Syntax

```
show dot1x quiet-period
```

To disable quiet time, use the no dot1x quiet-time command.

Parameters

seconds

Enter the number of seconds. The range is from 1 to 65535. The default is 60.

Defaults

60 seconds

Command Modes

INTERFACE

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
**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

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.0.0.0 | Introduced on the Z9000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the C-Series and S-Series.
7.4.1.0 | Introduced on the E-Series.
dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

Syntax

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

Parameters

- **number**: Enter the permitted number of re-authentications. The range is from 1 to 10. The default is 2.

Defaults

```
2
```

Command Modes

```
INTERFACE
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

dot1x server-timeout

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

Syntax

```
dot1x server-timeout seconds
```
To return to the default, use the `no dot1x server-timeout` command.

Parameters

- **seconds**: Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30.

Defaults

```
30 seconds
```

Command Modes

```
INTERFACE
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

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

Example

```plaintext
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 gigabitethernet 2/23
Dell(conf-if-gi-2/23)# dot1x server-timeout 40
Dell(conf-if-gi-2/23)#
```

dot1x static-mab

Enable static MAC authorization bypass (MAB) and configure static MAB profile to an interface.

**Syntax**

```
[no] dot1x static-mab profile profile-name
```

**Parameters**

`profile profile-name` Enter the keyword `profile` and the `profile-name` to configure the static MAB profile name. The profile name length is limited to 32 characters.

**Defaults**

Disabled.

**Command Modes**

INTERFACE

INTERFACE (BATCH MODE)
**Command History**

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S3100 series, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010.</td>
</tr>
</tbody>
</table>

**Usage Information**

The dot1x static-mab command enables static MAB (mac auth bypass) and configures the associated profile on a dot1x interface. Static MAB bypasses the authentication server for the supplicant MAC addresses configured in the associated profile.

Before you enable static MAB, you must do the following:

- Enable MAC authentication bypass on the port by configuring the dot1x mac-auth-bypass command.
- Ensure that no configured profile exists at the time of configuring the static-mab command.
- Use this command in Interface Batch Mode to enable static MAB in a dual-homing setup.

**Example**

Dell(conf)#do show dot1x interface ten gigabit ethernet 0/41

```
802.1x information on Te 0/41:
----------------------------------------
Dot1x Status:            Enable
Port Control:            AUTO
Port Auth Status:        AUTHORIZED (STATIC-MAB)
Re-Authentication:       Enable
Untagged VLAN id:        400
Guest VLAN:              Enable
Guest VLAN id:           400
Auth-Fail VLAN:          Enable
Auth-Fail VLAN id:       400
Auth-Fail Max-Attempts:  3
Critical VLAN:           Enable
Critical VLAN id:        400
Mac-Auth-Bypass:         Disable
Mac-Auth-Bypass Only:    Disable
Static-MAB:              Enable
Static-MAB Profile:      Sample
Tx Period:               30 seconds
Quiet Period:            60 seconds
ReAuth Max:              2
Supplicant Timeout:      30 seconds
Server Timeout:          30 seconds
Re-Auth Interval:        60 seconds
Max-EAP-Req:             2
Host Mode:               SINGLE_HOST
Auth PAE State:          Authenticated
Backend State:           Idle
```
Parameters

seconds Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30.

Defaults

30 seconds

Command Modes

INTERFACE

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

dot1x tx-period

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

Syntax

dot1x tx-period seconds

To return to the default, use the no dot1x tx-period command.

Parameters

seconds Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535. The default is 30.

Defaults

30 seconds

Command Modes

INTERFACE

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
mac

Configure a list of supplicant MAC addresses for dot1x profile represented with a profile-name.

Syntax

\[\text{[no]} \text{ mac \{mac-address1 mac-address2... mac-address6\}}\]

Parameters

- `mac-address1 mac-address2... mac-address6`: Enter the keyword `mac` and type the 48–bit MAC addresses using the H.H.H format. A maximum of 6 MAC addresses are allowed.

Defaults

None

Command Modes

- DOT1X PROFILE CONFIG (conf-dot1x-profile)
- CONFIGURATION TERMINAL BATCH

Command History

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010.</td>
</tr>
</tbody>
</table>

Usage Information

The `mac` command configures a list of supplicant MAC addresses for a dot1x profile represented with a profile-name. You can configure up to 6 MAC addresses in a single `mac` command. The maximum number of MAC addresses that you can configure in a single profile is limited to 100.

Use this command in Configuration Terminal Batch mode to configure a list of supplicant MAC addresses for dot1x profile in a dual-homing setup.

Example

```
Dell(conf)#dot1x profile mySupplicants
Dell(conf-dot1x-profile)#mac 00:50:56:AA:01:10 00:50:56:AA:01:11
Dell(conf-dot1x-profile)#show config
```
show dot1x cos-mapping interface

Display the CoS priority-mapping table the RADIUS server provides and applies to authenticated supplicants on an 802.1X-enabled system.

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

Parameters

- **interface**: Enter one of the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

- **mac-address**: (Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults
None

Command Modes
- EXEC
- EXEC privilege

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.4.2.1 Introduced on the C-Series and S-Series.

Usage Information
Enter a supplicant’s MAC address using the mac-address option to display CoS mapping information only for the specified supplicant.

You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in Single-Hot, Multi-Host, and Multi-Suppliant authentication modes.
show dot1x cos-mapping interface gigabitethernet 1/32

802.1p CoS re-map table on Gi 1/32:
----------------------------------
<table>
<thead>
<tr>
<th>Dot1p</th>
<th>Remapped Dot1p</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

show dot1x cos-mapping interface gigabitethernet 1/32 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 for Supplicant: 00:00:00:00:00:10
----------------------------------
<table>
<thead>
<tr>
<th>Dot1p</th>
<th>Remapped Dot1p</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

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 the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

- **mac-address**: (Optional) MAC address of a supplicant.

Defaults
None

Command Modes
- EXEC
- EXEC privilege

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

- **9.8(1.0)** Introduced on the Z9100-ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.2(1.0)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **9.0.0.0** Introduced on the Z9000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.12.0** Introduced on the S4810.
- **8.3.11.1** Introduced on the Z9000.
- **8.4.2.1** Added the `mac-address` option on the C-Series and S-Series.
- **7.6.1.0** Introduced on the C-Series, E-Series, and S-Series.

### Usage Information

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

#### Example

```bash
Dell# show dot1x interface gigabitethernet 1/32

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

#### Example (mac-address)

```bash
Dell# show dot1x interface gigabitethernet 1/32 mac-address 00:00:00:00:00:10

Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:

802.1x information on Gi 1/32:
-----------------------------
Dot1x Status:             Enable
Port Control:             AUTO
Port Auth Status:         AUTHORIZED(MAC-AUTH-BYPASS)
Re-Authentication:        Disable
Guest VLAN:               Enable
Guest VLAN id:            100
```
show dot1x profile

Display all the dot1x profiles or the details of a specific profile configured in the system.

Syntax

`show dot1x profile profile-name`

Parameters

- **profile-name**: Specify a static dot1x profile-name. The maximum character limit for a profile name is 32 characters.

show dot1x profile

**show dot1x**

Display all the dot1x profiles or the details of a specific profile configured in the system.

**Syntax**

`show dot1x profile profile-name`

**Parameters**

- **profile-name**: Specify a static dot1x profile-name. The maximum character limit for a profile name is 32 characters.
Defaults None
Command Modes EXEC
Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S3100 series, S4048-ON, S4048-ON, S4810, S4820T, S5000, S6000, S6000-ON, C9010, Z9100-ON, and Z9500.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010.</td>
</tr>
</tbody>
</table>

Example

Dell#show dot1x profile
802.1x profile information
--------------------------
Dot1x Profile mySupplicants
Profile MACs
  00:50:56:aa:01:10 00:50:56:aa:01:11
Access Control Lists (ACL)

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

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

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

NOTE: For ACL commands that use the Trace function, see Trace List Commands section in Security.

NOTE: For IPv6 ACL commands, see IPv6 Access Control Lists (IPv6 ACLs).

Topics:
- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Common MAC Access List Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands
- AS-Path Commands
- IP Community List Commands
- deny (for Standard IP ACLs)
- deny (for Extended IP ACLs)
- seq (for Standard IPv4 ACLs)
- deny tcp (for Extended IP ACLs)
- deny udp (for Extended IP ACLs)
- deny arp (for Extended MAC ACLs)
- deny icmp (for Extended IP ACLs)
- deny ether-type (for Extended MAC ACLs)
- deny (for Standard MAC ACLs)
- deny (for Extended MAC ACLs)
- permit (for Standard IP ACLs)
Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands in this chapter may use similar names, but require different options to support the different ACL types (for example, the **deny** and **permit** commands).

**remark**

Enter a description for an ACL entry.

Syntax

```
remark [remark-number] [description]
```

Parameters

- **remark-number**
  
  Enter the remark number. The range is from 0 to 65535 for MAC ACL and 0 to 4294967290 for IP ACL.

- **description**

  Enter a description of up to 80 characters.

Defaults

Not configured.

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version Description
- **9.8(1.0)** Introduced on the Z9100-ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.2(1.0)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.7.0** Introduced on the S4810.
- **8.1.1.0** Introduced on the E-Series.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.
- **6.4.1.0** Introduced on the E-Series.

### Usage Information
The `remark` command is available in each ACL mode. You can configure up to 4294967291 remarks for a given IP ACL and 65536 remarks for a given MAC ACL.

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.

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

! ip access-list standard test
 remark 5 Permit traffic from XYZ Inc.
 seq 5 permit 1.1.1.0/24
 remark 10 Deny rest of the traffic
 seq 10 deny any

Dell(config-std-nacl)#
```

### Related Commands
- `show config` — display the current ACL configuration.

### show config
Display the current ACL configuration.

#### Syntax
`show config`

#### Command Modes
- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED
### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2(1.1)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Example

```
Dell(config-std-nacl)# show conf
!
ip access-list standard test
  remark 5 Permit traffic from XYZ Inc.
  seq 5 permit 1.1.1.0/24 count
  remark 10 Deny traffic from ABC
  seq 10 deny 2.1.1.0/24 count
Dell(config-std-nacl)#
```

### Common IP ACL Commands

The following commands are available within both Ingress and Egress IP ACL modes (Standard and Extended) and do not have mode-specific options. When an ACL is created without a rule and then is applied to an interface, ACL behavior reflects an implicit permit. The platform supports both Ingress and Egress IP ACLs.

**NOTE:** Also refer to the Commands Common to all ACL Types section.

#### access-class

Apply a standard ACL to a terminal line.

**Syntax**

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

To remove an ACL, use the `no access-class` command.

**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

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0) Added the ipv4 and ipv6 parameters to the command.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.8.1.0 Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

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

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

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

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

Erase all counters maintained for access lists.

Syntax

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

Parameters

    access-list-name  (OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

Command Modes

    EXEC Privilege

Command History

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

Version                Description

    9.8(1.0)    Introduced on the Z9100-ON.
    9.8(0.0P5)  Introduced on the S4048-ON.
    9.8(0.0P2)  Introduced on the S3048-ON.
    9.7(0.0)    Introduced on the S6000-ON.
    9.2(1.0)    Introduced on the Z9500.
    9.0.2.0     Introduced on the S6000.
    8.3.19.0    Introduced on the S4820T.
    8.3.11.1    Introduced on the Z9000.
    8.3.7.0     Introduced on the S4810.
    8.1.1.0     Introduced on the E-Series.
    7.8.1.0     Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
    7.6.1.0     Introduced on the S-Series.
    7.5.1.0     Introduced on the C-Series.
    6.2.1.1     Introduced on the E-Series.

ip access-group

Assign an IP access list (IP ACL) to an interface.

Syntax

    ip access-group access-list-name {in | out} [implicit-permit] [vlan vlan-id] [vrf vrf-name]

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

Parameters

    access-list-name  Enter the name of a configured access list, up to 140 characters.
    in                Enter the keyword in to apply the ACL to incoming traffic.
    out               Enter the keyword out to apply the ACL to outgoing traffic.
implicit-permit (OPTIONAL) Enter the keyword implicit-permit to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).

vlan vlan-id (OPTIONAL) Enter the keyword vlan then the ID numbers of the VLANs. The range is from 1 to 4094 (you can use IDs from 1 to 4094).

vrf vrf-name (OPTIONAL) Enter the keyword vrf then the ID numbers of the VRFs. The range is from 1 to 63 (you can use IDs from 1 to 63).

NOTE: When you specify a single VRF, use the name of the VRF instead of the VRF ID number. Use the VRF ID numbers only when you specify a range of VRFs.

Defaults
Not enabled.

Command Modes INTERFACE/VRF MODE

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the S9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.8.1.0 Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Usage Information
You can assign one ingress ACL and one egress ACL to an interface.

NOTE: This command supports Loopback interfaces EE3 and EF series route processor modules (RPMs). This command does not support Loopback interfaces ED series RPMs and S-Series Loopback interfaces.

NOTE: If you apply outbound(egress) IP acl on a switch port, the filter applies only for routed traffic egressing out of that port.

To associate an access-list to a non-default VRF, use the vrf attribute of this command. You can use this command at the interface context (physical/LAG) to apply the access-list to a range of VRFs.

The VRF MODE is not available for the default and management VRFs.
ip control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv4 CPU traffic.

Syntax

ip control-plane egress-filter

Defaults
Not enabled.

Command Modes
EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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 [vrf vrf-name]

Parameters

access-list-name Enter the name of the ACL to be displayed.
cam_count List the count of the CAM rules for this ACL.
interface interface Enter the keyword interface then the one of the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a 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.
Identify whether ACL is applied on the ingress or egress side.

(Optional) Enter the keyword vrf and then the name of the VRF to view the IP accounting information on either a default or a non-default VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for the 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

- **NOTE:** The vrf option is available only when VRF feature is enabled.

```
show ip accounting access-lists
Field
"Extended IP..." Displays the name of the IP ACL.
"seq 5..." Displays the filter. If the keywords count or byte were configured in the filter, the number of packets or bytes the filter processes is displayed at the end of the line.
"order 4" Displays the QoS order of priority for the ACL entry.
```

Example

```
Dell# show ip accounting access-list L3-ACL vrf vrf3
!
Standard Ingress IP access list L3-ACL on vrf3
Total cam count 3
seq 5 permit 10.1.2.0/24
seq 10 permit 20.1.2.0/24
seq 15 permit 30.1.2.0/24
Dell#
```
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 | out] [vrf vrf-name]
```

**Parameters**

- `access-list-name` Enter the name of a configured MAC ACL, up to 140 characters.
- `interface interface` Enter the keyword interface followed by the one of the following keywords and slot/port or number information:
  - For a VLAN interface, enter the keyword vlan followed by the slot/port number.
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet followed by the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel followed by a number.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet followed by the slot/port information.
- `in | out` Identify whether ACL is applied on the ingress or egress side.
- `vrf vrf-name` Enter the keyword vrf and then the name of the VRF to display the access-lists that are configured on either the default or non-default VRFs.

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for the 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Standard IP ACL Commands**

When you create an ACL without any rule and then apply it to an interface, the ACL behavior reflects an implicit permit.

The platform supports both Ingress and Egress IP ACLs.

⚠️ **NOTE:** Also refer to the [Commands Common to all ACL Types](#) and [Common IP ACL Commands](#) sections.
deny

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

Syntax

deny {source | any | host {ip-address}} | no-drop

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {source [mask] | any | host ip-address} command.

Parameters

- **source**
  - Enter the IP address in dotted decimal format of the network from which the packet was sent.

- **any**
  - Enter the keyword any to specify that all routes are subject to the filter. You can enter any of the following keywords to specify route types.
    - `bytes` — Enter the keyword count to count packets the filter processes.
    - `count` — Enter the keyword byterorder to count bytes the filter processes.
    - `dscp` — Enter the keyword dscp followed by the DCSP value to match to the IP DCSCP values. The range is from 0 to 63.
    - `fragments` — Enter the keyword fragments to use ACLs to control packet fragments.
    - `order` — Enter the keyword order to specify the GoS order of priority for the ACL entry. The range is from 0 to 254 (0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). The default is, if you do not use the keyword order, the ACLs have the lowest order by default (255).

- **host ip-address**
  - Enter the keyword host and then enter the IP address to specify a host IP address only.

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

Defaults

Not configured.

Command Modes

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Access Control Lists (ACL) | 185
### Version Description

8.3.1.0  
Add the DSCP value for ACL matching.

8.2.1.0  
Allows ACL control of fragmented packets for IP (Layer 3) ACLs.

8.1.1.0  
Introduced on the E-Series.

7.6.1.0  
Introduced on the S-Series.

7.5.1.0  
Introduced on the C-Series.

7.4.1.0  
Added support for the non-contiguous mask and added the monitor option.

6.5.1.0  
Expanded to include the optional QoS order priority for the ACL entry.

#### Usage Information

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

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

#### Related Commands

- `ip access-list standard` — configure a standard ACL.
- `permit` — configure a permit filter.

---

### 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
```

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

**Parameters**

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

**Defaults**

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

**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**

9.8(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.

8.3.10.0  
Introduced on the S4810.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for the non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Networking OS supports one ingress and one egress IP ACL per interface.

Prior to Dell Networking OS version 7.8.1.0, names are up to 16 characters long.

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

**Example**

```
Dell(conf)# ip access-list standard TestList
Dell(config-std-nacl)#
```

**Related Commands**

- `ip access-list extended` — create an extended access list.
- `show config` — display the current configuration.

---

**permit**

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

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit {source [mask] | any | host ip-address}` command.

**Parameters**

- `source` Enter the IP address in dotted decimal format of the network from which the packet was sent.
- `mask` (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any` Enter the keyword `any` to specify that all routes are subject to the filter. You can enter any of the following keywords to specify route types.
  - `bytes` — Enter the keyword `bytes` to count bytes processed by the filter.
  - `count` — Enter the keyword `count` to count packets the filter processes.
  - `dscp` — Enter the keyword `dscp` to match to the IP DCSCP values.
  - `fragments` — Enter the keyword `fragments` to match to non-initial fragments of a datagram.
  - `order` — 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).
**Access Control Lists (ACL)**

**Syntax**

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

**Parameters**

- **ipv4 | ipv6 | mac**
  - Enter the keyword `ipv4` or `mac` to identify the access list type to resequence.

- **access-list-name**
  - Enter the name of a configured IP access list.

**Usage Information**

The `resequence` command does not resequence the existing rules. It reassigns sequence numbers to entries of an existing access-list.

**Related Commands**

- `deny` — assign a IP ACL filter to deny IP packets.
- `ip access-list standard` — create a standard ACL.

---

**Privilege Level**

- **Level** 15

**Default Configuration**

Not configured.

**Command Modes**

- **CONFIGURATION-STANDARD-ACCESS-LIST**

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Add the DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for the non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

---

**Usage Information**

The `no-drop` option is relevant in the context of the Policy QoS feature only. For more information, see the “Quality of Service” section of the Dell Networking OS Configuration Guide.

**Related Commands**

- `deny` — assign a IP ACL filter to deny IP packets.
- `ip access-list standard` — create a standard ACL.
StartingSeqNum Enter the starting sequence number to resequence. The range is from 0 to 4294967290.

Step-to-Increment Enter the step to increment the sequence number. The range is from 1 to 4294967290.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series (IPv6).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series (IPv4).</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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

seq

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

Syntax

```plaintext
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [no-drop]
```

To delete a filter, use the no seq sequence-number command.

Parameters

- **sequence-number**: Enter a number from 0 to 4294967290.
- **deny**: Enter the keyword deny to configure a filter to drop packets meeting this condition.
- **permit**: Enter the keyword permit to configure a filter to forward packets meeting this criteria.
source  Enter an IP address in dotted decimal format of the network from which the packet was received.

mask    (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

any     Enter the keyword any to specify that all routes are subject to the filter.

host ip-address Enter the keyword host then the IP address to specify a host IP address or hostname.

count   (OPTIONAL) Enter the keyword count to count packets the filter processes.

bytes   (OPTIONAL) Enter the keyword bytes to count bytes the filter processes.

dscp    (OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values.

order   (OPTIONAL) Enter the keyword order to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword order, the ACLs have the lowest order by default (255).

fragments Enter the keyword fragments to use ACLs to control packet fragments.

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

Defaults Not configured

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Add the DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for the non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>
The order option is relevant in the context of the Policy QoS feature only. The following applies:

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

**Related Commands**

- deny — configure a filter to drop packets.
- permit — configure a filter to forward packets.

## Extended IP ACL Commands

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

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

The platform supports both Ingress and Egress IP ACLs.

⚠️ **NOTE:** Also refer to the [Commands Common to all ACL Types](#) and [Common IP ACL Commands](#) sections.

### deny

Configure a filter that drops IP packets meeting the filter criteria.

**Syntax**

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- **ip**: Enter the keyword ip to configure a generic IP access list. The keyword ip specifies that the access list denies all IP protocols.
- **ip-protocol-number**: Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
- **source**: Enter the IP address of the network or host from which the packets were sent.
- **mask**: Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
- **any**: Enter the keyword any to specify that all routes are subject to the filter.
- **host ip-address**: Enter the keyword host then the IP address to specify a host IP address.
- **destination**: Enter the IP address of the network or host to which the packets are sent.
- **count**: (OPTIONAL) Enter the keyword count to count packets that the filter processes.
| **byte** | (OPTIONAL) Enter the keyword byte to count bytes that the filter processes. |
| **log** | (OPTIONAL, E-Series only) Enter the keyword log to enter ACL matches in the log. |
| **dscp** | (OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values. |
| **order** | (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword order, the ACLs have the lowest order by default (255). |
| **monitor** | (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, see Flow-based Monitoring in the Port Monitoring section in the Dell Networking OS Configuration Guide. |
| **fragments** | Enter the keyword fragments to use ACLs to control packet fragments. |
| **no-drop** | Enter the keywords no-drop to match only the forwarded packets. |

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th><strong>Version</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(10)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Add the DSCP value for ACL matching.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for the noncontiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

**Usage Information**

The order option is relevant in the context of the Policy GoS feature only. For more information, see the Quality of Service section in the Dell Networking OS Configuration Guide.
When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, see Port Monitoring.

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

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

**Related Commands**
- `deny tcp` — assign a filter to deny TCP packets.
- `deny udp` — assign a filter to deny UDP packets.
- `ip access-list extended` — create an extended ACL.

### deny icmp

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

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

To remove this filter, you have two choices:
- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**
- `source` Enter the IP address of the network or host from which the packets were sent.
- `mask` Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any` Enter the keyword `any` to specify that all routes are subject to the filter.
- `host ip-address` Enter the keyword `host` then the IP address to specify a host IP address.
- `destination` Enter the IP address of the network or host to which the packets are sent.
- `dscp` Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
- `count` (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- `byte` (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- `order` (OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
- `fragments` Enter the keyword `fragments` to use ACLs to control packet fragments.
- `no-drop` Enter the keywords `no-drop` to match only the forwarded packets.

**Defaults**
Not configured.
deny tcp

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

**Syntax**

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- **source**
  - Enter the IP address of the network or host from which the packets are sent.

- **mask**
  - Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any

Enter the keyword any to specify that all routes are subject to the filter.

host ip-address

Enter the keyword host then the IP address to specify a host IP address.

dscp

Enter this keyword dscp to deny a packet based on the DSCP value. The range is from 0 to 63.

bit

Enter a flag or combination of bits:

• ack: acknowledgement field
• fin: finish (no more data from the user)
• psh: push function
• rst: reset the connection
• syn: synchronize sequence numbers
• urg: urgent field

operator

(Optional) Enter one of the following logical operand:

• eq = equal to
• neq = not equal to
• gt = greater than
• lt = less than
• range = inclusive range of ports (you must specify two ports for the port command)

port port

Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.

The following list includes some common TCP port numbers:

• 23 = Telnet
• 20 and 21 = FTP
• 25 = SMTP
• 169 = SNMP

destination

Enter the IP address of the network or host to which the packets are sent.

mask

Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

count

(Optional) Enter the keyword count to count packets the filter processes.

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 did not use the keyword order, the ACLs have the lowest order by default (255).

fragments

Enter the keyword fragments to use ACLs to control packet fragments.

no-drop

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

Defaults

Not configured.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST
Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Added the keyword dscp.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Deprecated the keyword established.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Expanded to include the optional GoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>

Usage Information

The order option is relevant in the context of the Policy QoS feature only. For more information, see the Quality of Service section of the Dell Networking OS Configuration Guide.

The monitor option is relevant in the context of flow-based monitoring only. For more information, see the Port Monitoring section.

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

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

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000111110100000</td>
<td>1111111111100000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111000000</td>
<td>1111111111100000</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000</td>
<td>1111100000000000</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000</td>
<td>1111100000000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001111000000000</td>
<td>1111111000000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111100000000</td>
<td>1111111110000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
</tbody>
</table>
An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>000000000000000 111111100000000 0</td>
<td>1023 1024</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Ports: 1024

Related Commands
- `deny` — assign a filter to deny IP traffic.
- `deny udp` — assign a filter to deny UDP traffic.

deny udp

To drop user datagram protocol (UDP) packets meeting the filter criteria, configure a filter.

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

To remove this filter, you have two choices:
- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters
- `source` Enter the IP address of the network or host from which the packets were sent.
- `mask` Enter a network mask in /prefix format (/X) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any` Enter the keyword any to specify that all routes are subject to the filter.
- `host ip-address` Enter the keyword host then the IP address to specify a host IP address.
- `dscp` Enter this keyword dscp to deny a packet based on the DSCP value. The range is from 0 to 63.
- `operator` (OPTIONAL) Enter one of the following logical operand:
  - `eq` = equal to
  - `neq` = not equal to
  - `gt` = greater than
  - `lt` = less than
  - `range` = inclusive range of ports (you must specify two ports for the port command)
- `port port` Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
- `destination` Enter the IP address of the network or host to which the packets are sent.
mask  Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

count  (OPTIONAL) Enter the keyword count to count packets processed by the filter.

byte  (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.

order  (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword order, the ACLs have the lowest order by default (255).

fragments  Enter the keyword fragments to use ACLs to control packet fragments.

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

Defaults  Not configured.

Command Modes  CONFIGURATION-EXTENDED-ACCESS-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the keyword dscp.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the monitor option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Deprecated the keyword established.</td>
</tr>
</tbody>
</table>

Usage Information  The order option is relevant in the context of the Policy GoS feature only. For more information, see the Quality of Service section of the Dell Networking OS Configuration Guide.

The monitor option is relevant in the context of flow-based monitoring only. For more information, see the Port Monitoring section.
The C-Series and S-Series cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

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

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

**Example**

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule#   Data                    Mask       From To #Covered
1 0000111111010000 1111111111100000 4000 4031 32
2 0000111111010000 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 1111111111000000 8000 8000 1
Total Ports: 4001
```

**Example**

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule#   Data                    Mask       From To #Covered
1 0000000000000000 1111110000000000 0 1023 1024
Total Ports: 1024
```

**Related Commands**

- `deny` — assign a filter to deny IP traffic.
- `deny tcp` — assign a filter to deny TCP traffic.

### ip access-list extended

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

**Syntax**

```
ip access-list extended access-list-name
```

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

**Parameters**

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

**Defaults**

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

**Command Modes**

CONFIGURATION

**Command History**

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

**Version**

- 9.8(1.0)
  - Introduced on the Z9100-ON.
- 9.8(0.0P5)
  - Introduced on the S4048-ON.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Expanded to accept up to 140 chars.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

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

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

**Example**

```
Dell(conf)# ip access-list extended TESTListEXTEND
Dell(config-ext-nacl)#
```

**Related Commands**

- `ip access-list standard` — configure a standard IP access list.
- `show config` — display the current configuration.

---

### permit

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

**Syntax**

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- `source`: Enter the IP address in dotted decimal format of the network from which the packet was sent.
- `mask`: (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any`: Enter the keyword `any` to specify that all routes are subject to the filter.
- `host ip-address`: Enter the keyword `host` then the IP address to specify a host IP address or hostname.
destination  Enter the IP address of the network or host to which the packets are sent.
count (OPTIONAL) Enter the keyword count to count packets processed by the filter.
bytes (OPTIONAL) Enter the keyword bytes to count bytes processed by the filter.
dscp  (OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values.
order (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry.
The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword order, the ACLs have the lowest order by default (255).
fragments Enter the keyword fragments to use ACLs to control packet fragments.
no-drop Enter the keywords no-drop to match only the forwarded packets.

Defaults
Not configured.

Command Modes
CONFIGURATION-EXTENDED-ACCESS-LIST

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0) Added the no-drop parameter.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.3.1.0 Added the DSCP value for ACL matching.
8.2.1.0 Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.11.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
7.4.1.0 Added support for the non-contiguous mask and added the monitor option.
6.5.10 Expanded to include the optional QoS order priority for the ACL entry.

Usage Information
The order option is relevant in the context of the Policy GoS feature only. For more information, see the “Quality of Service” section of the Dell Networking OS Configuration Guide.

The software cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.
Related Commands

- **ip access-list extended** — create an extended ACL.
- **permit tcp** — assign a permit filter for TCP packets.
- **permit udp** — assign a permit filter for UDP packets.

**permit tcp**

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

**Syntax**

```plaintext
permit tcp (source mask | any | host ip-address) [bit] [operator port [port]] (destination mask | any | host ip-address) [bit] [dscp] [operator port [port]] [count [byte] [order] [fragments] [no-drop]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- **source**
  - Enter the IP address of the network or host from which the packets were sent.
- **mask**
  - Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- **any**
  - Enter the keyword `any` to specify that all routes are subject to the filter.
- **host ip-address**
  - Enter the keyword `host` then the IP address to specify a host IP address.
- **bit**
  - Enter a flag or combination of bits:
    - `ack`: acknowledgement field
    - `fin`: finish (no more data from the user)
    - `psh`: push function
    - `rst`: reset the connection
    - `syn`: synchronize sequence numbers
    - `urg`: urgent field
- **dscp**
  - Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
- **operator**
  - (OPTIONAL) Enter one of the following logical operand:
    - `eq`: equal to
    - `neq`: not equal to
    - `gt`: greater than
    - `lt`: less than
    - `range`: inclusive range of ports (you must specify two ports for the port parameter)
- **port port**
  - Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535.
  - The following list includes some common TCP port numbers:
    - `23`: Telnet
- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

**destination**
Enter the IP address of the network or host to which the packets are sent.

**mask**
Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

**count**
(Optional) Enter the keyword count to count packets the filter processes.

**byte**
(Optional) Enter the keyword byte to count bytes the filter processes.

**order**
(Optional) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword order, the ACLs have the lowest order by default (255).

**fragments**
Enter the keyword fragments to use ACLs to control packet fragments.

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

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION-EXTENDED-ACCESS-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the keyword dscp.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Allows ACL control of fragmented packets for IP (Layer 3) ACLs.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added support for non-contiguous mask and added the monitor option. Deprecated the keyword established.</td>
</tr>
<tr>
<td>6.5.10</td>
<td>Expanded to include the optional QoS order priority for the ACL entry.</td>
</tr>
</tbody>
</table>
Usage Information

The order option is relevant in the context of the Policy QoS feature only. For more information, see the “Quality of Service” section of the Dell Networking OS Configuration Guide.

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

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

The monitor option is relevant in the context of flow-based monitoring only. For more information, see the Port Monitoring section.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Data</th>
<th>Mask</th>
<th>From To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000111110100000</td>
<td>1111111111000000</td>
<td>4000 4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000111111110000</td>
<td>1111111110000000</td>
<td>4032 4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0001000000000000</td>
<td>1111100000000000</td>
<td>4096 6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0001100000000000</td>
<td>1111100000000000</td>
<td>6144 7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0001110000000000</td>
<td>1111110000000000</td>
<td>7168 7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0001111000000000</td>
<td>1111111000000000</td>
<td>7680 7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0001111100000000</td>
<td>1111111100000000</td>
<td>7936 7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0001111101000000</td>
<td>1111111111000000</td>
<td>8000 8000</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Ports: 4001

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Data</th>
<th>Mask</th>
<th>From To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000</td>
<td>1111110000000000</td>
<td>0 1023</td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

Related Commands

- `ip access-list extended` — create an extended ACL.
- `permit` — assign a permit filter for IP packets.
- `permit udp` — assign a permit filter for UDP packets.

permit udp

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

Syntax

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

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit udp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.`
Parameters

source Enter the IP address of the network or host from which the packets were sent.

mask Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

any Enter the keyword any to specify that all routes are subject to the filter.

host ip-address Enter the keyword host and then enter the IP address to specify a host IP address.

dscp Enter the keyword dscp to deny a packet based on the DSCP value. The range is from 0 to 63.

operator (OPTIONAL) Enter one of the following logical operand:

- eq = equal to
- neq = not equal to
- gt = greater than
- lt = less than
- range = inclusive range of ports (you must specify two ports for the port parameter)

port port Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is 0 to 65535.

destination Enter the IP address of the network or host to which the packets are sent.

count (OPTIONAL) Enter the keyword count to count packets processed by the filter.

byte (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.

order (OPTIONAL) Enter the keyword order to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword order, the ACLs have the lowest order by default (255).

fragments Enter the keyword fragments to use ACLs to control packet fragments.

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

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0) Added the no-drop parameter.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
### Version Description
- **8.3.1.0**: Added the keyword `dscp`.
- **8.2.1.0**: Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
- **8.1.1.0**: Introduced on the E-Series.
- **7.6.1.0**: Introduced on the S-Series.
- **7.5.1.0**: Introduced on the C-Series.
- **7.4.1.0**: Added support for non-contiguous mask and added the `monitor` option.
- **6.5.10**: Expanded to include the optional QoS `order` priority for the ACL entry.

### Usage Information
The `order` option is relevant in the context of the Policy GoS feature only. For more information, see the “Quality of Service” section of the Dell Networking OS Configuration Guide.

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

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

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

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, `gt`, `lt`, or `range`) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

### Example
An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>4000</td>
<td>4031</td>
<td>32</td>
</tr>
<tr>
<td>2</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>4032</td>
<td>4095</td>
<td>64</td>
</tr>
<tr>
<td>3</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>4096</td>
<td>6143</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>6144</td>
<td>7167</td>
<td>1024</td>
</tr>
<tr>
<td>5</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>7168</td>
<td>7679</td>
<td>512</td>
</tr>
<tr>
<td>6</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>7680</td>
<td>7935</td>
<td>256</td>
</tr>
<tr>
<td>7</td>
<td>0000000000000000</td>
<td>1111111111000000</td>
<td>7936</td>
<td>7999</td>
<td>64</td>
</tr>
<tr>
<td>8</td>
<td>0000000000000000</td>
<td>1111111111111111</td>
<td>8000</td>
<td>8000</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Ports: 4001

### Example
An ACL rule with a TCP port `lt 1023` uses only one entry in the CAM.

<table>
<thead>
<tr>
<th>Rule#</th>
<th>Data</th>
<th>Mask</th>
<th>From</th>
<th>To</th>
<th>#Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0000000000000000</td>
<td>1111111000000000</td>
<td>0</td>
<td>1023</td>
<td>1024</td>
</tr>
</tbody>
</table>

Total Ports: 1024

### Related Commands
- `ip access-list extended` — create an extended ACL.
- `permit` — assign a permit filter for IP packets.
- `permit tcp` — assign a permit filter for TCP packets.
resequence access-list

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

Syntax

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

Parameters

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

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series (IPv4).</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

When all sequence numbers are exhausted, this feature permits re-assigning a new sequence number to entries of an existing access-list.
Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

**Syntax**

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp | ip | tcp | udp} 
{source mask | any | host ip-address} 
{destination mask | any | host ip-address} 
{operator port [port]} 
[count [byte] | log] 
[dscp value] 
[order] 
[monitor] 
[fragments] 
[no-drop]
```

**Parameters**

- `sequence-number` Enter a number from 0 to 4294967290.
- `deny` Enter the keyword deny to configure a filter to drop packets meeting this condition.
- `permit` Enter the keyword permit to configure a filter to forward packets meeting this criteria.
- `ip-protocol-number` Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
- `icmp` Enter the keyword icmp to configure an ICMP access list filter.
- `ip` Enter the keyword ip to configure a generic IP access list. The keyword ip specifies that the access list permits all IP protocols.
- `tcp` Enter the keyword tcp to configure a TCP access list filter.
- `udp` Enter the keyword udp to configure a UDP access list filter.
- `source` Enter an IP address in dotted decimal format of the network from which the packet was received.
- `mask` (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
- `any` Enter the keyword any to specify that all routes are subject to the filter.
- `host ip-address` Enter the keyword host and then enter the IP address to specify a host IP address or hostname.
- `operator` (OPTIONAL) Enter one of the following logical operands:
  - `eq` = equal to
  - `neq` = not equal to
  - `gt` = greater than
  - `lt` = less than
  - `range` = inclusive range of ports (you must specify two ports for the port parameter.)
- `port port` (OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535.
  The following list includes some common TCP port numbers:
  - 23 = Telnet
  - 20 and 21 = FTP
  - 25 = SMTP
  - 169 = SNMP
- `destination` Enter the IP address of the network or host to which the packets are sent.
- `count` (OPTIONAL) Enter the keyword count to count packets the filter processes.
byte  (OPTIONAL) Enter the keyword byte to count bytes the filter processes.

log  (OPTIONAL, E-Series only) Enter the keyword log to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.

dscp  (OPTIONAL) Enter the keyword dscp to match to the IP DCSCP values.

order  (OPTIONAL) Enter the keyword order to specify the GoS 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).

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.

fragments  Enter the keyword fragments to use ACLs to control packet fragments.

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

Defaults  Not configured

Command Modes  CONFIGURATION-EXTENDED-ACCESS-LIST

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

Version  Description
9.8(1.0)  Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.8(0.0)  Added the no-drop parameter.
9.7(0.0)  Introduced on the S6000-ON.
9.2(1.0)  Introduced on the Z9500.
9.0.2.0  Introduced on the S6000.
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.3.7.0  Introduced on the S4810.
8.3.1.0  Add the DSCP value for ACL matching.
8.2.1.0  Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0  Introduced on the E-Series.
7.6.1.0  Introduced on the S-Series.
7.5.1.0  Introduced on the C-Series.
7.4.1.0  Added support for the non-contiguous mask and added the monitor option. Deprecated the keyword established.
6.5.10  Expanded to include the optional QoS order priority for the ACL entry.

NOTE: For more information, see “Flow-based Monitoring” in the Port Monitoring section of the Dell Networking OS Configuration Guide.
Usage Information

The monitor option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

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

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

When you use the log option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

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

Related Commands

- deny — configure a filter to drop packets.
- permit — configure a filter to forward packets.

Common MAC Access List Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options. These commands allow you to clear, display, and assign MAC ACL configurations.

The platform supports both Ingress and Egress MAC ACLs.

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

**clear counters mac access-group**

Clear counters for all or a specific MAC ACL.

**Syntax**

```plaintext
clear counters mac access-group [mac-list-name]
```

**Parameters**

- **mac-list-name** (OPTIONAL) Enter the name of a configured MAC access list.

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. You can apply a MAC ACL on a physical, port-channel, or VLAN interface.

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.

| NOTE: This option is available only with the keyword in option.

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.

optimized Enter the keyword optimized to enable ACL optimization.

in Enter the keyword in to configure the ACL to filter incoming traffic.

out Enter the keyword out to configure the ACL to filter outgoing traffic.

| NOTE: 1. If the MAC ACL is applied on VLAN, none of the VLAN members should have an access list applied for that VLAN.

2. If the MAC ACL is applied on a Physical or Port Channel interface, the VLAN in which this port is associated should not have an access list applied.

3. If the MAC ACL is applied on a VLAN, then that VLAN should not belong to VLAN ACL group.

4. If the MAC ACL is applied on a VLAN ACL group, then none of the VLANs in that group should have an access list applied on it.
Defaults

Command Modes

Command History

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

Usage Information

You can assign one ingress ACL and one egress ACL (standard or extended) to an interface.

Related Commands

- `mac access-list standard` — configure a standard MAC ACL.

- `mac access-list extended` — configure 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 the interface information:

  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.

  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.
For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.

Identify whether ACL is applied on ingress or egress side.

**Command Modes**
- EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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 the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a 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.

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

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

Standard MAC ACL Commands

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

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

To drop packets with a the MAC address specified, configure a filter.

Syntax
deny {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log] [monitor]

To remove this filter, you have two choices:
- Use the no seq sequence-number command if you know the filter’s sequence number.
Use the `no deny {any | mac-source-address mac-source-address-mask}` command.

**Parameters**
- **any**: Enter the keyword `any` to specify that all routes are subject to the filter.
- **mac-source-address**: Enter a MAC address in nn:nn:nn:nn:nn:nn format.
- **mac-source-address-mask** (OPTIONAL): Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
- **count** (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- **byte** (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- **log** (OPTIONAL, E-Series only) Enter the keyword `log` to log the packets.
- **monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, see the "Flow-based Monitoring" in the Port Monitoring section in the Dell Networking OS Configuration Guide.

**Defaults**
Not enabled.

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added the <code>monitor</code> option.</td>
</tr>
</tbody>
</table>

**Usage Information**
When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

**Related Commands**
- `permit` — configures a MAC address filter to pass packets.
- `seq` — configures a MAC address filter with a specified sequence number.
mac access-list standard

To configure a standard MAC ACL, name a new or existing MAC access control list (MAC ACL) and enter MAC ACCESS LIST mode. Also refer to the Commands Common to all ACL Types section and the Common MAC Access List Commands section.

Syntax

mac access-list standard mac-list-name
To delete a MAC access list, use the no mac access-list standard mac-list-name command.

Parameters

mac-list-name
Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults
Not configured.

Command Modes
CONFIGURATION

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

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.8.1.0 Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.1.1.0 Introduced on the E-Series.

Usage Information
Dell Networking OS supports one ingress and one egress MAC ACL per interface.

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

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

Example

Dell(conf)# mac-access-list access-list standard TestMAC
Dell(config-std-macl)# permit 00:00:00:00:00:00 00:00:00:ff:ff count
Dell(config-std-macl)# deny any count
Dell(config-std-macl)#
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.
- `mac-source-address-mask` (OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
- `count` (OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
- `byte` (OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
- `log` (OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
- `threshold-in msgs count` (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, see “Flow-based Monitoring” in the Port Monitoring section of the Dell Networking OS Configuration Guide.

Defaults

- Not configured.

Command Modes

- CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version Description
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.1.1.0 Introduced on the E-Series.

Usage Information
When you use the log option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

Related Commands
- deny — configure a MAC ACL filter to drop packets.
- seq — configure a MAC ACL filter with a specified sequence number.

**seq**

To deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

**Syntax**
```
deny {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:
- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {any | mac-source-address mac-source-address-mask} command.

**Parameters**
- **any** Enter the keyword any to specify that all routes are subject to the filter.
- **mac-source-address** Enter a MAC address in nn:nn:nn:nn:nn:nn format.
- **mac-source-address-mask** (OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
- **count** (OPTIONAL) Enter the keyword count to count packets processed by the filter.
- **byte** (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.
- **log** (OPTIONAL) Enter the keyword log to include ACL messages in the log.
- **threshold-in-msgs** (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- **interval minutes** (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
- **monitor** (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the
monitored interface. For more information, see “Flow-based Monitoring” in the Port Monitoring section in the Dell Networking OS Configuration Guide.

**Defaults**  
Not configured

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added the monitor option.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**  
When you use the log option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

**Related Commands**  
- deny — configure a filter to drop packets.
- permit — configure a filter to forward packets.

---

**Extended MAC ACL Commands**

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

The platform supports both Ingress and Egress MAC ACLs.

**NOTE:** For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.
deny

To drop packets that match the filter criteria, configure a filter.

Syntax

deny {any | host mac-address | mac-source-address mac-source-address-mask} {any |
host mac-address | mac-destination-address mac-destination-address-mask} [ethertype-operator] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} command.

Parameters

- **any**
  - Enter the keyword any to drop all packets.

- **host mac-address**
  - Enter the keyword host and then enter a MAC address to drop packets with that host address.

- **mac-source-address**

- **mac-source-address-mask**
  - Specify which bits in the MAC address must match.
  - The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

- **mac-destination-address**
  - Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

- **mac-destination-address-mask**
  - Specify which bits in the MAC address must match.
  - The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

- **ethertype operator**
  - (OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes:
    - **ev2** - is the Ethernet II frame format
    - **llc** - is the IEEE 802.3 frame format
    - **snap** - is the IEEE 802.3 SNAP frame format

- **count**
  - (OPTIONAL) Enter the keyword count to count packets processed by the filter.

- **byte**
  - (OPTIONAL) Enter the keyword byte to count bytes processed by the filter.

- **log**
  - (OPTIONAL) Enter the keyword log to include ACL messages in the log.

- **threshold-inmsgs count**
  - (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
interval minutes  (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.

monitor  (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, see “Flow-based Monitoring” in the Port Monitoring section of the Dell Networking OS Configuration Guide.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added the monitor option.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information When you use the log option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

Related Commands

- permit — configure a MAC address filter to pass packets.
- seq — configure 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]
```

To delete a MAC access list, use the no mac access-list extended access-list-name command.
Parameters

- **access-list-name**: Enter a text string as the MAC access list name, up to 140 characters.
- **cpu-qos**: Enter the keywords `cpu-qos` to assign this ACL to control plane traffic only (CoPP).

Defaults

None

Command Modes

CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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

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

Example

```
Dell(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 gig 1/17 in
Extended mac access-list snickers on GigabitEthernet 1/17
seq 10 permit any any ev2 eq 800 count bytes (559851886 packets 191402152148 bytes)
seq 20 permit any any ev2 eq 806 count bytes (74481486 packets 5031686754 bytes)
seq 30 permit any any ev2 eq 86dd count bytes (7751519 packets 797843521 bytes)
```

Related Commands

- `mac access-list standard` — configure a standard MAC access list.
• show mac accounting access-list — display MAC access list configurations and counters (if configured).

**permit**

To pass packets matching the criteria specified, configure a filter.

**Syntax**

```
permit {any | host mac-address | mac-source-address mac-source-address-mask} 
{any | host mac-address | mac-destination-address mac-destination-address-mask} 
[ethertype operator] [count [byte]] | [log] [monitor]
```

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no permit {any | host mac-address | mac-source-address mac-source-address-mask} {any | mac-destination-address mac-destination-address-mask} command.

**Parameters**

- **any**
  Enter the keyword any to forward all packets.

- **host**
  Enter the keyword host then a MAC address to forward packets with that host address.

- **mac-source-address**

- **mac-source-address-mask**
  (OPTIONAL) Specify which bits in the MAC address must match.

  The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

- **mac-destination-address**
  Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

- **mac-destination-address-mask**
  Specify which bits in the MAC address must be matched.

  The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.

- **ethertype operator**
  (OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes:
  
  - ev2 - is the Ethernet II frame format
  - llc - is the IEEE 802.3 frame format
  - snap - is the IEEE 802.3 SNAP frame format

- **count**
  (OPTIONAL) Enter the keyword count to count packets the filter processes.

- **byte**
  (OPTIONAL) Enter the keyword byte to count bytes the filter processes.

- **log**
  (OPTIONAL, E-Series only) Enter the keyword log to log the packets.

- **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.

**NOTE:** For more information, see Flow-based Monitoring in the “Port Monitoring” section of the *Dell Networking OS Configuration Guide.*
Defaults
Not configured.

Command Modes
CONFIGURATION-MAC ACCESS LIST-EXTENDED

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
7.4.1.0 Added the monitor option.
6.1.1.0 Introduced on the E-Series.

Usage Information
When you use the log option, the CP processor logs details about the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets’ details.

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

Related Commands
- deny — configure a MAC ACL filter to drop packets.
- seq — configure a MAC ACL filter with a specified sequence number.

IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. To configure or enable IP prefix lists, use these commands.

clear ip prefix-list

Reset the number of times traffic meets the conditions ("hit" counters) of the configured prefix lists.

Syntax

```
clear ip prefix-list [prefix-name]
```
Parameters

prefix-name  (OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.

Defaults

Clears “hit” counters for all prefix lists unless a prefix list is specified.

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- ip prefix-list — configure a prefix list.

deny

To drop packets meeting the criteria specified, configure a filter.

Syntax

deny ip-prefix [ge min-prefix-length] [le max-prefix-length]

To delete a drop filter, use the no deny ip-prefix command.

Parameters

ip-prefix  Specify an IP prefix in the network/length format. For example, 35.0.0.0/ 8 means match the first 8 bits of address 35.0.0.0.

ge min-prefix-length  (OPTIONAL) Enter the keyword ge and then enter the minimum prefix length, which is a number from zero (0) to 32.

le max-prefix-length  (OPTIONAL) Enter the keyword le and then enter the maximum prefix length, which is a number from zero (0) to 32.
Defaults
Not configured.

Command Modes
PREFIX-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
Sequence numbers for this filter are automatically assigned starting at sequence number 5.

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

**ip prefix-list**

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

**Syntax**

```
ip prefix-list prefix-name
```

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

**Parameters**

- `prefix-name` Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Usage Information

Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Related Commands

- `show ip route list` — display IP routes in an IP prefix list.
- `show ip prefix-list summary` — display a summary of the configured prefix lists.

```
seq
```

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

```
seq sequence-number [deny | permit] [any] [ip-prefix /nn [ge min-prefix-length] [le max-prefix-length]] [bitmask number]
```

Parameters

- `sequence-number` Enter a number. The range is from 1 to 4294967294.
- `deny` Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
- `permit` Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
- `any` (OPTIONAL) Enter the keyword `any` to match any packets.
- `ip-prefix /nn` (OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
- `ge min-prefix-length` (OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
- `le max-prefix-length` (OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.
- `bitmask number` Enter the keyword `bitmask` then enter a bit mask number in dotted decimal format.

Defaults

- Not configured.
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the bit mask option.</td>
</tr>
</tbody>
</table>

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

show config
Display the current PREFIX-LIST configurations.

Syntax
show config

Command Modes
PREFIX-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
**Version** | **Description**
--- | ---
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.1.1.0 | Introduced on the E-Series.

**Example**

Dell(conf-nprefixl)# show config
!
ip prefix-list snickers
Dell(conf-nprefixl)#

### show ip prefix-list detail

Display details of the configured prefix lists.

**Syntax**

```
show ip prefix-list detail [prefix-name]
```

**Parameters**

- `prefix-name` (OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) |Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.8.1.0 | Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.1.1.0 | Introduced on the E-Series.

**Example**

Dell# show ip prefix-list detail
Ip Prefix-list with the last deletion/insertion: PL_OSPF_to_RIP
show ip prefix-list summary

Display a summary of the configured prefix lists.

Syntax

show ip prefix-list summary [prefix-name]

Parameters

prefix-name  (OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

• EXEC
• EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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
Dell#
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.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `continue` feature allows movement from one route-map entry to a specific route-map entry (the sequence number). If you do not specify the sequence number, the `continue` feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the `continue` feature executes only after a successful match occurs. If there are no successful matches, the `continue` feature is ignored.

**Match clause with Continue clause**

The `continue` feature can exist without a match clause. A `continue` clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a `continue` clause, the match clause executes first and the `continue` clause next in a specified route map entry. The `continue` clause launches only after a successful match. The behavior is:
• A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
• If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
• If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

**Set Clause with Continue Clause**

If the route-map entry contains sets with the continue clause, set actions are performed first then the continue clause jumps to the specified route map entry.

• If a set action occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same set command.
• If set community additive and set as-path prepend are configure, the communities and AS numbers are prepended.

**Related Commands**

- **set community** — specify a COMMUNITY attribute.
- **set as-path** — configure a filter to modify the AS path.

### description

Add a description to this route map.

**Syntax**

description {description}

To remove the description, use the no description {description} command.

**Parameters**

description

Enter a description to identify the route map (80 characters maximum).

**Defaults**

None

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
match as-path

To match routes that have a certain AS number in their BGP path, configure a filter.

Syntax

    match as-path as-path-name

To delete a match AS path filter, use the no match as-path as-path-name command.

Parameters

    as-path-name

    Enter the name of an established AS-PATH ACL, up to 140 characters.

Defaults

    Not configured.

Command Modes

    ROUTE-MAP

Command History

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

    Version Description
    9.8(1.0) Introduced on the Z9100–ON.
    9.8(0.0P5) Introduced on the S4048-ON.
    9.8(0.0P2) Introduced on the S3048-ON.
    9.7(0.0) Introduced on the S6000–ON.
    9.2(1.0) Introduced on the Z9500.
    9.0.2.0 Introduced on the S6000.
    8.3.19.0 Introduced on the S4820T.
    8.3.11.1 Introduced on the Z9000.
    8.3.7.0 Introduced on the S4810.
    8.1.1.0 Introduced on the E-Series.
    7.8.1.0 Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
    7.6.1.0 Introduced on the S-Series.
    7.5.1.0 Introduced on the C-Series.
    pre-6.1.1.0 Introduced on the E-Series.

Related Commands

    • set as-path — add information to the BGP AS_PATH attribute.
**match community**

To match routes that have a certain COMMUNITY attribute in their BGP path, configure a filter.

**Syntax**

```plaintext
match community community-list-name [exact]
```

To delete a community match filter, use the `no match community` command.

**Parameters**

- `community-list-name` Enter the name of a configured community list.
- `exact` (OPTIONAL) Enter the keywords `exact` to process only those routes with this community list name.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `set community` — specify a COMMUNITY attribute.

**match interface**

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

**Syntax**

```plaintext
match interface interface
```

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

**interface**

Enter the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match ip address` — redistribute routes that match an IP address.
- `match ip next-hop` — redistribute routes that match the next-hop IP address.
- `match ip route-source` — redistribute routes that match routes advertised by other routers.
- `match metric` — redistribute routes that match a specific metric.
- `match route-type` — redistribute routes that match a route type.
- `match tag` — redistribute routes that match a specific tag.
**match ip address**

To match routes based on IP addresses specified in an access list, configure a filter.

**Syntax**

```
match ip address prefix-list-name
```

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

**Parameters**

- `prefix-list-name` Enter the name of configured prefix list, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match interface` — redistribute routes that match the next-hop interface.
- `match ip next-hop` — redistribute routes that match the next-hop IP address.
- `match ip route-source` — redistribute routes that match routes advertised by other routers.
- `match metric` — redistribute routes that match a specific metric.
- `match route-type` — redistribute routes that match a route type.
- `match tag` — redistribute routes that match a specific tag.
**match ip next-hop**

To match based on the next-hop IP addresses specified in an IP access list or IP prefix list, configure a filter.

**Syntax**

```
match ip next-hop {prefix-list prefix-list-name}
```

To delete a match, use the `no match ip next-hop {prefix-list prefix-list-name}` command.

**Parameters**

- `prefix-list prefix-list-name`: Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match interface` — redistribute routes that match the next-hop interface.
- `match ip address` — redistribute routes that match an IP address.
- `match ip route-source` — redistribute routes that match routes advertised by other routers.
- `match metric` — redistribute routes that match a specific metric.
- `match route-type` — redistribute routes that match a route type.
- `match tag` — redistribute 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 {prefix-list prefix-list-name}
```

To delete a match, use the `no match ip route-source {prefix-list prefix-list-name}` command.

**Parameters**

- `prefix-list prefix-list-name`  
Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match interface` — redistribute routes that match the next-hop interface.
- `match ip address` — redistribute routes that match an IP address.
- `match ip next-hop` — redistribute routes that match the next-hop IP address.
- `match metric` — redistribute routes that match a specific metric.
- `match route-type` — redistribute routes that match a route type.
- `match tag` — redistribute 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

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

    Version     Description
    9.8(1.0)    Introduced on the Z9100–ON.
    9.8(0.0P5)  Introduced on the S4048-ON.
    9.8(0.0P2)  Introduced on the S3048-ON.
    9.7(0.0)    Introduced on the S6000-ON.
    9.2(1.0)    Introduced on the Z9500.
    9.0.2.0     Introduced on the S6000.
    8.3.19.0    Introduced on the S4820T.
    8.3.11.1    Introduced on the Z9000.
    8.3.7.0     Introduced on the S4810.
    8.1.1.0     Introduced on the E-Series.
    7.6.1.0     Introduced on the S-Series.
    7.5.1.0     Introduced on the C-Series.
    pre-6.1.1.0 Introduced on the E-Series.

Related Commands
    • match interface — redistribute routes that match the next-hop interface.
    • match ip address — redistribute routes that match an IP address.
    • match ip next-hop — redistribute routes that match the next-hop IP address.
    • match ip route-source — redistribute routes that match routes advertised by other routers.
    • match route-type — redistribute routes that match a route type.
    • match tag — redistribute routes that match a specific tag.
```

**match origin**

To match routes based on the value found in the BGP path ORIGIN attribute, configure a filter.

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

**Parameters**
- **egp**
  - Enter the keyword `egp` to match routes originating outside the AS.
- **igp**
  - Enter the keyword `igp` to match routes originating within the same AS.
- **incomplete**
  - Enter the keyword `incomplete` to match routes with incomplete routing information.

**Defaults**
- Not configured.

**Command Modes**
- `ROUTE-MAP`

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---

**match route-type**

To match routes based on the how the route is defined, configure a filter.

**Syntax**
```
match route-type {external [type-1 | type-2] | internal | level-1 | level-2 | local}
```

To delete a match, use the `no match route-type {local | internal | external [type-1 | type-2] | level-1 | level-2}` command.

**Parameters**
- **external [type-1 | type-2]**
  - Enter the keyword `external` then either `type-1` or `type-2` to match only on OSPF Type 1 routes or OSPF Type 2 routes.
- **internal**
  - Enter the keyword `internal` to match only on routes generated within OSPF areas.
- **level-1**
  - Enter the keyword `level-1` to match IS-IS Level 1 routes.
- **level-2**
  - Enter the keyword `level-2` to match IS-IS Level 2 routes.
- **local**
  - Enter the keyword `local` to match only on routes generated within the switch.

**Defaults**
- Not configured.
To redistribute only routes that match a specified tag value, configure a filter.

**Syntax**

```plaintext
match tag tag-value
```

To remove a match, use the `no match tag` command.

**Parameters**

- **tag-value**
  Enter a value as the tag on which to match. The range is from zero (0) to 4294967295.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match interface` — redistribute routes that match the next-hop interface.
- `match ip address` — redistribute routes that match an IP address.
- `match ip next-hop` — redistribute routes that match the next-hop IP address.
- `match ip route-source` — redistribute routes that match routes advertised by other routers.
- `match metric` — redistribute routes that match a specific metric.
- `match tag` — redistribute routes that match a specific tag.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `match interface` — redistribute routes that match the next-hop interface.
- `match ip address` — redistribute routes that match an IP address.
- `match ip next-hop` — redistribute routes that match the next-hop IP address.
- `match ip route-source` — redistribute routes that match routes advertised by other routers.
- `match metric` — redistribute routes that match a specific metric.
- `match route-type` — redistribute 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.

```
route-map map-name [permit | deny] [sequence-number]
```

To delete a route map, use the `no route-map map-name [permit | deny] [sequence-number]` command.

**Parameters**

- `map-name` Enter a text string of up to 140 characters to name the route map for easy identification.
- `permit` (OPTIONAL) Enter the keyword `permit` to set the route map default as permit. If you do not specify a keyword, the default is `permit`.
- `deny` (OPTIONAL) Enter the keyword `deny` to set the route map default as deny.
- `sequence-number` (OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. The range is from 1 to 65535.

**Defaults**

Not configured. If you do not define a keyword (`permit` or `deny`) for the route map, the `permit` action is the default.

**Command Modes**

CONFIGURATION
Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same map-name are deleted when you use the no route-map map-name command.

Example

Dell(conf)# route-map dempsey
Dell(config-route-map)#

Related Commands

• show config — display the current configuration.

set as-path

To modify the AS path for border gateway protocol (BGP) routes, configure a filter.

Syntax

    set as-path prepend as-number [...] as-number

To remove an AS-Path setting, use the no set as-path {prepend as-number | tag} command.

Parameters

prepend as-number Enter the keyword prepend and then enter up to eight AS numbers to be inserted into the BGP path information. The range is from 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

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

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

**Syntax**

```
set automatic-tag
```

To return to the default, enter `no set automatic-tag`.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

**Related Commands**

- `match as-path` — redistribute routes that match an AS-PATH attribute.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `set level` — specify the OSPF area for route redistribution.
- `set metric` — specify the metric value assigned to redistributed routes.
- `set metric-type` — specify the metric type assigned to redistributed routes.
- `set tag` — specify the tag assigned to redistributed routes.

**set comm-list delete**

To remove the specified community list from the BGP route’s COMMUNITY attribute, configure a filter.

**Syntax**

```
set comm-list community-list-name delete
```

To insert the community list into the COMMUNITY attribute, use the `no set comm-list community-list-name delete` command.

**Parameters**

- `community-list-name` Enter the name of an established Community list, up to 140 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
7.8.1.0 | Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.0 | Introduced on the E-Series.

Usage Information

The community list used in the `set comm-list delete` command must be configured so that each filter contains only one community. For example, the filter `deny 100:12` is acceptable, but the filter `deny 120:13 140:33` results in an error.

If the `set comm-list delete` command and the `set community` command are configured in the same route map sequence, the deletion command (`set comm-list delete`) is processed before the insertion command (`set community`).

Related Commands

- `match community` — redistribute routes that match the COMMUNITY attribute.
- `set community` — specify a COMMUNITY attribute.

**set community**

Allows you to assign a BGP COMMUNITY attribute.

**Syntax**

```
set community {community-number | local-as | no-advertise | no-export | none} [additive]
```

To delete a BGP COMMUNITY attribute assignment, use the `no set community {community-number | local-as | no-advertise | no-export | none}` command.

**Parameters**

- `community-number` Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
- `local-AS` Enter the keywords `local-AS` to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED.
  All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
- `no-advertise` Enter the keywords `no-advertise` to drop all routes containing the well-known community attribute of NO_ADVERTISE.
  All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
- `no-export` Enter the keywords `no-export` to drop all routes containing the well-known community attribute of NO_EXPORT.
  All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
- `none` Enter the keyword `none` to remove the community attribute from routes meeting the route map criteria.
additive

(Optionalal) Enter the keyword additive to add the communities to already existing communities.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- match community — redistribute routes that match the COMMUNITY attribute.
- show ip bgp community — display BGP community groups.

**set level**

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

**Syntax**

```
set level {backbone | level-1 | level-1-2 | level-2 | stub-area}
```

To remove a set level condition, use the `no set level {backbone | level-1 | level-1-2 | level-2 | stub-area}` command.

**Parameters**

- **backbone**

  Enter the keyword backbone to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).

- **level-1**

  Enter the keyword level-1 to redistribute matched routes to IS-IS Level 1.

- **level-1-2**

  Enter the keyword level-1-2 to redistribute matched routes to IS-IS Level 1 and Level 2.

- **level-2**

  Enter the keyword level-2 to redistribute matched routes to IS-IS Level 2.

- **stub-area**

  Enter the keyword stub to redistribute matched routes to OSPF stub areas.
set local-preference

To set the BGP LOCAL_PREF attribute for routers within the local autonomous system, configure a filter.

Syntax

```
set local-preference value
```

To delete a BGP LOCAL_PREF attribute, use the `no set local-preference` command.

Parameters

- **value**
  
Enter a number as the LOCAL_PREF attribute value. The range is from 0 to 4294967295.

Defaults

Not configured.

Command Modes

- ROUTE-MAP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `set automatic-tag` — compute the tag value of the route.
- `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.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**  
The `set local-preference` command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the `bgp default local-preference` command.

**Related Commands**  
- `bgp default local-preference` — change the default LOCAL_PREF attribute for all routes.

---

### set metric

To assign a new metric to redistributed routes, configure a filter.

**Syntax**  
```
set metric [+] metric-value
```

To delete a setting, enter `no set metric`.

**Parameters**
- `+` (OPTIONAL) Enter + to add a metric-value to the redistributed routes.
- `-` (OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.
- `metric-value`  
  Enter a number as the new metric value. The range is from zero (0) to 4294967295.

**Defaults**  
Not configured.

**Command Modes**  
ROUTE-MAP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
set metric-type

To assign a new route type for routes redistributed to OSPF, configure a filter.

Syntax

```
set metric-type {internal | external | type-1 | type-2}
```

To delete a setting, use the `no set metric-type` command.

Parameters

- **internal**: Enter the keyword `internal` to assign the Interior Gateway Protocol metric of the next hop as the route’s BGP MULTI_EXIT_DES (MED) value.
- **external**: Enter the keyword `external` to assign the IS-IS external metric.
- **type-1**: Enter the keyword `type-1` to assign the OSPF Type 1 metric.
- **type-2**: Enter the keyword `type-2` to assign the OSPF Type 2 metric.

Defaults

Not configured.

Command Modes

```
ROUTE-MAP
```

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.3.1.0 | Implemented the keyword `internal`.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.0 | Introduced on the E-Series.

Related Commands
- `set automatic-tag` — compute the tag value of the route.
- `set level` — specify the OSPF area for route redistribution.
- `set metric` — specify the metric value assigned to redistributed routes.
- `set tag` — specify the tag assigned to redistributed routes.

**set next-hop**

To specify an IP address as the next hop, configure a filter.

**Syntax**
```
set next-hop ip-address
```

To delete the setting, use the `no set next-hop ip-address` command.

**Parameters**
- `ip-address` Specify an IP address in dotted decimal format.

**Defaults**
Not configured.

**Command Modes**
ROUTE-MAP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
**Version** | **Description**
--- | ---
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.0 | Introduced on the E-Series.

**Usage Information**

If you configure the `set next-hop` command, its configuration takes precedence over the `neighbor next-hop-self` command in the ROUTER BGP mode.

If you configure the `set next-hop` command with the interface's IP address (either Loopback or physical), the software declares the route unreachable.

**Related Commands**

- `match ip next-hop` — redistribute routes that match the next-hop IP address.

### set origin

To manipulate the BGP ORIGIN attribute, configure a filter.

**Syntax**

```plaintext
set origin {igp | egp | incomplete}
```

To delete an ORIGIN attribute setting, use the `no set origin` command.

**Parameters**

- `egp` Enter the keyword `egp` to set routes originating from outside the local AS.
- `igp` Enter the keyword `igp` to set routes originating within the same AS.
- `incomplete` Enter the keyword `incomplete` to set routes with incomplete routing information.

**Defaults**

Not configured.

**Command Modes**

ROUTE-MAP

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
set tag

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

Syntax

```
set tag tag-value
```

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

Parameters

- **tag-value**: Enter a number as the tag. The range is from zero (0) to 4294967295.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `set automatic-tag` — compute the tag value of the route.
- `set level` — specify the OSPF area for route redistribution.
- `set metric` — specify the metric value assigned to redistributed routes.
- `set metric-type` — specify the route type assigned to redistributed routes.
**set weight**

To add a non-RFC compliant attribute to the BGP route to assist with route selection, configure a filter.

**Syntax**

```
set weight weight
```

To delete a weight specification, use the `no set weight weight` command.

**Parameters**

- **weight**
  
  Enter a number as the weight used by the route meeting the route map specification. The range is from 0 to 65535. The default is router-originated = 32768 and all other routes = 0.
  
  When there are multiple routes to the same destination, the routes with a higher weight are preferred.

**Defaults**

- router-originated = 32768; all other routes = 0

**Command Modes**

- ROUTE-MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(10)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>pre-6.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you do not use the `set weight` command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

**show config**

Display the current route map configuration.

**Syntax**

```
show config
```

254 | Access Control Lists (ACL)
show route-map

Display the current route map configurations.

Syntax 
show route-map [map-name]

Parameters 

map-name 
(OPTIONAL) Enter the name of a configured route map, up to 140 characters.

Command Modes 

EXEC 
EXEC Privilege

Command History 

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

Example

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

AS-Path Commands

The following commands configure AS-Path ACLs.

ip as-path access-list

Enter AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

Syntax

ip as-path access-list as-path-name

Parameters

as-path-name Enter the access-list name, up to 140 characters.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

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

Version Description

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

9.8(0.0P2) Introduced on the S3048-ON.
### Access Control Lists (ACL)

**Version** | **Description**
--- | ---
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.8.1.0 | Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
pre-Version 6.1.1.0 | Introduced on the E-Series.

**Usage Information**
To apply the AS-PATH ACL to BGP routes, use the `match as-path` or `neighbor filter-list` commands.

**Example**
```
Dell(conf)# ip as-path access-list TestPath
Dell(config-as-path)#
```

**Related Commands**
- `match as-path` — match on routes contain a specific AS-PATH.

### show ip as-path-access-lists

Display the all AS-PATH access lists configured on the E-Series.

**Syntax**
```
show ip as-path-access-lists
```

**Command Modes**
- EXEC
- EXEC Privilege

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

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
pre-Version 6.1.1.0 | Introduced on the E-Series.

**Example**
```
Dell# show ip as-path-access-lists
ip as-path access-list acc
   permit 750
   deny 10
Dell#
```
IP Community List Commands

IP community list commands are supported on the Dell Networking OS.

ip community-list

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

Syntax

```
ip community-list comm-list-name
```

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

Parameters

- `comm-list-name` Enter a text string as the name of the community-list, up to 140 characters.

Command Modes

- CONFIGURATION

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Example

```
Dell(conf)# ip community-list TestComList
Dell(config-community-list)#
```

show ip community-lists

Display configured IP community lists in alphabetic order.

Syntax

```
show ip community-lists [name]
```

Parameters

- `name` (OPTIONAL) Enter the name of the standard or extended IP community list, up to 140 characters.

Command Modes

- EXEC
**deny (for Standard IP ACLs)**

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

**Syntax**
```
deny {source | any | host {ip-address}} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:
- Use the `no seq` `sequence-number` command if you know the filter’s sequence number.
- Use the `no deny {source [mask] | any | host ip-address}` command.

**Parameters**

- `log` *(OPTIONAL)* Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in-msgs count` *(OPTIONAL)* Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` *(OPTIONAL)* Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
- `monitor` *(OPTIONAL)* Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.
The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**
CONFIGURATION-STANDARD-ACCESS-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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` — configure a standard ACL.
- `permit` — configure a permit filter.

**deny (for Extended IP ACLs)**
Configure a filter that drops IP packets meeting the filter criteria.

**Syntax**
```plaintext
deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [byte]] [dscp value] [order] [monitor] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
Use the no deny {ip | ip-protocol-number} (source mask | any | host ip-address)
(destination mask | any | host ip-address) command.

Parameters

- **log** (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- **threshold-in msgs count** (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- **interval minutes** (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
- **monitor** (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

- **CONFIGURATION-EXTENDED-ACCESS-LIST**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

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` — assign a filter to deny TCP packets.
- `deny udp` — assign a filter to deny UDP packets.
- `ip access-list extended` — create an extended ACL.

seq (for Standard IPv4 ACLs)

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

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

- `log` (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- `threshold-in-msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

- `CONFIGURATION-STANDARD-ACCESS-LIST`

Command History

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

Version Description

- **9.8(1.0)** Introduced on the Z9100–ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2）** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000–ON.
- **9.4(0.0)** Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
- **9.3(0.0)** Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists.

This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

- deny — configure a filter to drop packets.
- permit — configure a filter to forward packets.

deny tcp (for Extended IP ACLs)

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

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator port [port]]
    {destination mask | any | host ip-address} [dscp] [bit] [operator port [port]]
    [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs
    count]] [monitor]
```

Parameters

- **log** (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- **threshold-in msgs count** (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- **interval minutes** (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- **monitor** (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.
The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

### Command Modes

**CONFIGURATION-EXTENDED-ACCESS-LIST**

### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added the support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

### 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** — assign a filter to deny IP traffic.
- **deny udp** — assign a filter to deny UDP traffic.

---

**deny udp (for Extended IP ACLs)**

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] [log [interval minutes] [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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>(OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.</td>
</tr>
<tr>
<td>threshold-in msgs</td>
<td>(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.</td>
</tr>
<tr>
<td>count</td>
<td>(OPTIONAL) Enter the keyword count followed by a value to indicate ACL logs must be generated, the time interval range is from 1 to 10 minutes.</td>
</tr>
<tr>
<td>interval minutes</td>
<td>(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.</td>
</tr>
</tbody>
</table>

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.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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

Version     Description

9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.3(0.0)    Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

Related Commands

-   **deny** — assign a filter to deny IP traffic.
-   **deny tcp** — assign 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**

- **log** *(OPTIONAL)* Enter the keyword `log` to enable the triggering of ACL log messages.
- **threshold-in msgs** *(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.
- **count** *(OPTIONAL)* Enter the keyword `count` 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`

**Command History**

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

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.4(0.0) | Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.5(0.1) | Introduced on the Z9500.
9.3(0.0) | Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism
copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny icmp (for Extended IP ACLs)

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

NOTE: Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

Syntax

deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} {dscp} [message-type] [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} command.

Parameters

log

(Optional) Enter the keyword log to enable the triggering of ACL log messages.

threshold-in-msgs count

(Optional) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.

interval minutes

(Optional) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.

monitor

(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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

Version Description

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

9.8(0.0P2) Introduced on the S3048-ON.

9.3(0.0) Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

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

```plaintext
deny ether-type protocol-type-number {destination-mac-address mac-address-mask [any]} vlan vlan-id {source-mac-address mac-address-mask [any]} [count [byte]] [order] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no deny ether-type protocol-type-number {destination-mac-address mac-address-mask [any]} vlan vlan-id {source-mac-address mac-address-mask [any]}` command.

Parameters

- `log` (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- `threshold-in msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

- By default, 10 ACL logs are generated if you do not specify the threshold explicitly.
- The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

Usage Information
When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny (for Standard MAC ACLs)
To drop packets with a the MAC address specified, configure a filter.

Syntax
deny {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log [interval minutes] [threshold-in-msgs [count]][monitor]

To remove this filter, you have two choices:
- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {any | mac-source-address mac-source-address-mask} command.

Parameters
log
(Optional) Enter the keyword log to enable the triggering of ACL log messages.
threshold-in msgs
(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.
count
(Optional) Enter the keyword count followed by a value to indicate that the count (drop or byte) counters are maintained for ACLs.
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.
(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-MAC ACCESS LIST-STANDARD`

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.4(0.0) | Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0) | Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

**Related Commands**

- `permit` — configure a MAC address filter to pass packets.
- `seq` — configure a MAC address filter with a specified sequence number.
deny (for Extended MAC ACLs)

To drop packets that match the filter criteria, configure a filter.

Syntax

deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} [ethertype-operator] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no deny {any | host mac-address | mac-source-address mac-source-address-mask} {any | host mac-address | mac-destination-address mac-destination-address-mask} command.

Parameters

- log
  (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.

- threshold-in-msgs count
  (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. The threshold range is from 1 to 100.

- interval minutes
  (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.

- monitor
  (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.
The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

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 counts for the new interval is initialized. If the maximum threshold is exceeded within an interval, all the logs for that interval are deleted to prevent excessive memory usage.

When flow-based monitoring is enabled through the flow-based enable command, a flow record is created for a packet only if the MAC ACL deny rule at the tail end of the ACL contains the monitor option.

The flow-based enable command is not applicable for MAC ACLs. As a result, when you enter the flow-based enable command, it is ignored instead of generating a syslog message.

Similarly, when you de-enable the flow-based enable command, it is ignored instead of generating a syslog message.

When you configure ACL logging and byte counters simultaneously, byte counters may display incorrect values. Configure packet counters instead of byte counters.

When ACL logging is configured for a policy map and you enable monitoring, packet ACL logging information is not accounted in the ACL log output for those rules which are common in both the policy maps.
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** — configure a MAC address filter to pass packets.
- **seq** — configure 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**

```plaintext
permit {source [mask] | any | host ip-address} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter's sequence number.
- Use the no permit {source [mask] | any | host ip-address} command.

**Parameters**

- **log** *(OPTIONAL)* Enter the keyword log to enable the triggering of ACL log messages.
- **threshold-in-msgs** *(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.
- **count** *(OPTIONAL)* Enter the count keyword followed by a number to indicate the maximum number of ACL logs that can be generated. The 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 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-STD-ACCESS-LIST**

272 | Access Control Lists (ACL)
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

### 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` — assign a IP ACL filter to deny IP packets.
- `ip access-list standard` — create a standard ACL.

### permit arp (for Extended MAC ACLs)

Configure a filter that forwards ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

#### Syntax

```
permit arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]][monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `{destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

#### Parameters

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs count

(Optional) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.

interval minutes

(Optional) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

monitor

(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0) Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).
permit ether-type (for Extended MAC ACLs)

Configure a filter that allows traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

Syntax

```
permit ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} [count [byte]] [order] [log [interval minutes] [threshold-in msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter's sequence number.
- Use the no permit ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} command.

Parameters

- `log`  
  (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.

- `threshold-in msgs count`  
  (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. The threshold range is from 1 to 100.

- `interval minutes`  
  (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

- `monitor`  
  (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

- **CONFIGURATION-EXTENDED-ACCESS-LIST**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.
If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

### permit icmp (for Extended IP ACLs)

Configure a filter to allow all or specific ICMP messages.

**Syntax**

```
permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} [dscp] [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in-msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

CONFIGURATION-STANDARD-ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
</tbody>
</table>
Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

**permit udp (for Extended IP ACLs)**

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

```
permit udp {source mask | any | host ip-address} [operator port [port]]
{destination mask | any | host ip-address} [dscp] [operator port [port]] [count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- **log**
  - (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

- **threshold-inmsgs count**
  - (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

- **interval minutes**
  - (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
(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`

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3.0.0</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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` — create an extended ACL.
- `permit` — assign a permit filter for IP packets.
- `permit tcp` — assign a permit filter for TCP packets.
permit (for Extended IP ACLs)

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

**Syntax**

```
permit {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes]] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

**Parameters**

- **log** (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- **threshold-in msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- **interval minutes** (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- **monitor** (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added the support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.
If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, standard and extended IPv6 ACLs, and standard and extended MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

**Related Commands**

- `ip access-list extended` — create an extended ACL.
- `permit tcp` — assign a permit filter for TCP packets.
- `permit udp` — assign a permit filter for UDP packets.

### permit (for Standard MAC ACLs)

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

**Syntax**

```
permit {any | mac-source-address [mac-source-address-mask]} [count [byte]] | [log [interval minutes] | [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

**Parameters**

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in-msgs` (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.
- `count` (OPTIONAL) Enter the keyword `count` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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** — configure a MAC ACL filter to drop packets.
- **seq** — configure a MAC ACL filter with a specified sequence number.

seq (for Standard MAC ACLs)

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

**Syntax**

```
seq sequence-number {deny | permit} {any | mac-source-address [mac-source-address-mask]} [count {byte}] [log [interval minutes] [threshold-in-msgs count] [monitor]
```

To remove this filter, use the no seq sequence-number command.

**Parameters**

- **log** (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- **threshold-in-msgs count** (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- **interval minutes** (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
(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-MAC ACCESS LIST-STANDARD`

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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` — configure a filter to drop packets.
- `permit` — configure a filter to forward packets.
permit tcp (for Extended IP ACLs)

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

Syntax

```
permit tcp {source mask | any | host ip-address} [bit] [operator port [port]]
(destination mask | any | host ip-address) [bit] [dscp] [operator port [port]]
[count [byte]] [order] [fragments] [log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter’s sequence number.
- Use the no permit tcp {source mask | any | host ip-address} {destination mask |
  any | host ip-address} command.

Parameters

- **log** (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- **threshold-in-msgs** (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.
- **count** (OPTIONAL) Enter the keyword count 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-EXTENDED-ACCESS-LIST**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

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` — create an extended ACL.
- `permit` — assign a permit filter for IP packets.
- `permit udp` — assign a permit filter for UDP packets.

seq arp (for Extended MAC ACLs)

Configure an egress filter with a sequence number that filters ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

**NOTE:** Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

**Syntax**

```
seq sequence-number {deny | permit} arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count [byte]] [order] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, use the no seq sequence-number command.

**Parameters**

- `log` *(OPTIONAL)* Enter the keyword log to enable the triggering of ACL log messages.
- `threshold-in-msgs` *(OPTIONAL)* Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. You can enter a threshold in the range of 1-100.
- `interval minutes` *(OPTIONAL)* Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.
- `monitor` *(OPTIONAL)* Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.
Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, Z9000, and MXL 10/40GbE Switch IO Module platforms.</td>
</tr>
<tr>
<td>9.3.0.0</td>
<td>Added support for logging of ACLs on the S4810, S4820T, Z9000, and MXL 10/40GbE Switch IO Module platforms.</td>
</tr>
</tbody>
</table>

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is reenabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is reenabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, standard and extended IPv6 ACLs, and standard and extended MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

seq ether-type (for Extended MAC ACLs)

Configure an egress filter with a specific sequence number that filters traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

**NOTE:** Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

**Syntax**

```
seq sequence-number {deny | permit} ether-type protocol-type-number
(destination-mac-address mac-address-mask | any) vlan vlan-id (source-mac-address mac-address-mask | any) [count [byte]] [order] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

**Parameters**

- `log` (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.

To remove this filter, use the no seq sequence-number command.
threshold-in msgs count

(Optional) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. You can enter a threshold in the range of 1-100.

interval minutes

(Optional) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.

monitor

(Optional) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

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

Version Description

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

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000–ON.

9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, Z9000, and MXL 10/40GbE Switch IO Module platforms.

9.3.0.0 Added support for logging of ACLs on the S4810, S4820T, Z9000, and MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is reenabled for this new interval.

If ACL logging was stopped because the configured threshold is exceeded, it is reenabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, standard and extended IPv6 ACLs, and standard and extended MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead 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).
seq (for IP ACLs)

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

**Syntax**

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp | ip | tcp | udp} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator port [port]] [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

**Parameters**

- `log` (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- `threshold-in-msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

CONFIGURATION-EXTENDED-ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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` — configure a filter to drop packets.
- `permit` — configure a filter to forward packets.

### seq (for IPv6 ACLs)

Assign a sequence number to a deny or permit the filter in an IPv6 access list while creating the filter.

**Syntax**
```
seq sequence-number {deny | permit} {ipv6-protocol-number | icmp | ip | tcp | udp} {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [operator port [port]] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

**Parameters**
- `log` (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- `threshold-in msgs` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminate with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

**Defaults**
By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes** ACCESS-LIST

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

### 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` — configure a filter to forward packets.

### permit udp (for IPv6 ACLs)

Configure a filter to pass UDP packets meeting the filter criteria.

**Syntax**

```plaintext
permit udp {source address mask | any | host ipv6-address} [operator port [port]] {destination address | any | host ipv6-address} [operator port [port]] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

**Parameters**

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in-msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3.0.0</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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 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).

**permit tcp (for IPv6 ACLs)**

Configure a filter to pass TCP packets that match the filter criteria.

**Syntax**

```
permit tcp {source address mask | any | host ipv6-address} [operator port [port]] {destination address | any | host ipv6-address} [bit] [operator port [port]] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter’s sequence number.
Use the no permit tcp (source address mask | any | host ipv6-address) (destination address | any | host ipv6-address) command.

Parameters

- log (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- threshold-in-msgs count (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- interval minutes (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- monitor (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.4(0.0) Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0) Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging was 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 – assign a permit filter for IP packets.

permit icmp (for IPv6 ACLs)

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax

    permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]]] [monitor]

To remove this filter, you have two choices:

- Use the no seq sequence-number command if you know the filter's sequence number.
- Use the no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} command.

Parameters

- log (OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.
- threshold-in-msgs count (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- interval minutes (OPTIONAL) Enter the keyword interval followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- monitor (OPTIONAL) Enter the keyword monitor when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

**permit (for IPv6 ACLs)**

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

**Syntax**

```plaintext
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor] [no-drop]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number command syntax if you know the filter’s sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

**Parameters**

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in-msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
- `no-drop` Enter the keywords `no-drop` to match only the forwarded packets.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.
The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**Usage Information**

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny udp (for IPv6 ACLs)

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

**Syntax**

deny udp {source address mask | any | host ipv6-address} [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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>(OPTIONAL) Enter the keyword log to enable the triggering of ACL log messages.</td>
</tr>
<tr>
<td>threshold-in msgs count</td>
<td>(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.</td>
</tr>
<tr>
<td>interval minutes</td>
<td>(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.</td>
</tr>
<tr>
<td>monitor</td>
<td>(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.</td>
</tr>
</tbody>
</table>

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, Z9000, and MXL 10/40GbE Switch IO Module platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, Z9000, and MXL 10/40GbE Switch IO Module platforms.</td>
</tr>
</tbody>
</table>

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs.

You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and
egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny tcp (for IPv6 ACLs)

Configure a filter that drops TCP packets that match the filter criteria.

Syntax

```
deny tcp {source address mask | any | host ipv6-address} [operator port [port]]
{destination address | any | host ipv6-address} [bit] [operator port [port]]
[count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number
- Use the `no deny tcp {source address mask | any | host ipv6-address}
{destination address | any | host ipv6-address} command`

Parameters

- `log` (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- `threshold-in msgs count` (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated, with the seq, permit, or deny commands. The threshold range is from 1 to 100.
- `interval minutes` (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
- `monitor` (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
</tbody>
</table>
Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny icmp (for Extended IPv6 ACLs)

Configure a filter to drop all or specific ICMP messages.

**NOTE:** Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

Syntax

```
deny icmp {source address mask | any | host ipv6-address} {destination address
| any | host ipv6-address} [message-type] [count [byte]] | [log [interval
minutes] [threshold-in-msgs [count]]] [monitor]
```

To remove this filter, you have two choices:

- Use the no seq sequence-number command syntax if you know the filter's sequence number
- Use the no deny icmp {source address mask | any | host ipv6-address}
  {destination address | any | host ipv6-address} command

**Parameters**

- **log**
  
  (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

- **threshold-in-msgs count**
  
  (OPTIONAL) Enter the threshold-in-msgs keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. You can enter a threshold in the range of 1-100.

- **interval minutes**
  
  (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.

- **monitor**
  
  (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.
By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

**ACCESS-LIST**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are generated 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 was 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 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).

**deny (for IPv6 ACLs)**

Configure a filter that drops IPv6 packets that match the filter criteria.

**Syntax**

```plaintext
deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor] [no-drop]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter’s sequence number.

**deny**

Configure a filter that drops IPv6 packets that match the filter criteria.

**Syntax**

```plaintext
deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor] [no-drop]
```
Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} command` to disable deny rules.

**Parameters**

- **log** (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
- **threshold-in-msgs count** (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. 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.
- **no-drop** Enter the keywords `no-drop` to match only the forwarded packets.

**Defaults**

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

**Command Modes**

- ACCESS-LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the no-drop parameter.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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 was 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.
egress direction. Flow-based monitoring conserves bandwidth by monitoring only 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).
This section describes the access control list (ACL) virtual local area network (VLAN) group, and content addressable memory (CAM) enhancements.

**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)

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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.

Syntax

```
ip access-group {group name} out implicit-permit
```

Parameters

- **group-name**
  - Enter the name of the ACL VLAN group where you want the egress IP ACLs applied, up to 140 characters.
- **out**
  - Enter the keyword out to apply the ACL to outgoing traffic.
- **implicit-permit**
  - Enter the keyword implicit-permit to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).

Default

None

Command Modes

- CONFIGURATION (conf-acl-vl-grp)

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3,(0.0)</td>
<td>Introduced on the S4810, S4820T, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

Usage Information

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.

Syntax

```
show acl-vlan-group {group-name | detail}
```

Parameters

- **group-name**
  - (Optional) Display only the ACL VLAN group that is specified, up to 140 characters.
- **detail**
  - 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.

Default

No default behavior or values

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3.(0.0)</td>
<td>Introduced on the S4810, S4820T, Z9000 and MXL platforms</td>
</tr>
</tbody>
</table>

**Usage Information**

When an ACL-VLAN-Group name or the Access List Group Name contains more than 30 characters, the name is truncated in the show acl-vlan-group command output.

### Examples

The following sample illustrates the output of the show acl-vlan-group 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    Egress IP Acl     Ingress IP Acl     Ingress V6 Acl      Vlan
Members
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    Egress IP Acl     Ingress IP Acl     Ingress IPv6 Acl
Vlan Members
Test             -                 test                -                 1-100
```

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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.3.(0.0) | Introduced on the S4810, S4820T, Z9000 and MXL platforms

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis Vlan Cam ACL</td>
<td>Details about the CAM blocks allocated for ACLs for various VLAN operations at a system-wide, global level.</td>
</tr>
<tr>
<td>Stack Unit &lt;number&gt;</td>
<td>Details about the CAM blocks allocated for ACLs for various VLAN operations for a particular stack unit.</td>
</tr>
<tr>
<td>Current Settings(in block sizes)</td>
<td>Information about the number of FP blocks that are currently in use or allocated.</td>
</tr>
<tr>
<td>VlanOpenFlow</td>
<td>Number of FP blocks for VLAN open flow operations.</td>
</tr>
<tr>
<td>VlanIscsi</td>
<td>Number of FP blocks for VLAN internet small computer system interface (iSCSI) counters.</td>
</tr>
<tr>
<td>VlanHp</td>
<td>Number of FP blocks for VLAN high performance processes.</td>
</tr>
<tr>
<td>VlanFcoe</td>
<td>Number of FP blocks for VLAN Fiber Channel over Ethernet (FCoE) operations.</td>
</tr>
<tr>
<td>VlanAclOpt</td>
<td>Number of FP blocks for ACL VLAN optimization feature.</td>
</tr>
</tbody>
</table>

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
Dell#
```

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> |vlanaclopt <0-2>
```

**Parameters**

- `default` | 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.
- `vlanopenflow <0-2>` | Allocate the number of FP blocks for VLAN open flow operations.
- `vlaniscsi <0-2>` | Allocate the number of FP blocks for VLAN ISCSI counters.
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

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

**Version** | **Description**
---|---
9.8(0.0P5)| Introduced on the S4048-ON.
9.8(0.0P2)| Introduced on the S3048-ON.
9.5(0.1)| Introduced on the Z9500.
9.3(0.0)| Introduced on the S4810 and Z9000 platforms.

**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 IPv4 Flow 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

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

**Version** | **Description**
---|---
9.8(0.0P5)| Introduced on the S4048-ON.
9.8(0.0P2)| Introduced on the S3048-ON.
9.3(0.0)| Introduced on the S4810, S4820T, Z9000 and MXL platforms.
The following regions must be provided in the `show cam-usage` output:

- L3AclCam
- L2AclCam
- V6AclCam

The following table describes the output fields of this `show` command:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StackUnit</td>
<td>The Stack unit number</td>
</tr>
<tr>
<td>Portpipe</td>
<td>The hardware path that packets follow through a system for ACL optimization</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>Type of area in the CAM block that is used for ACL VLAN groups</td>
</tr>
<tr>
<td>Total CAM</td>
<td>Total amount of space in the CAM block</td>
</tr>
<tr>
<td>Used CAM</td>
<td>Amount of CAM space that is currently in use</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Amount of CAM space that is free and remaining to be allocated for ACLs</td>
</tr>
</tbody>
</table>

**Example 1:** Output of the `show cam-usage` Command

```
Dell#show cam-usage
Stackunit|Portpipe| CAM Partition   | Total CAM   |  Used CAM   | Available CAM
========|========|=================|=============|=============|==============
1   |   0    | IN-L2 ACL       |      1536   |         0    |      1536
|        | IN-L3 ACL       |      1024   |         1    |      1023
|        | IN-L3 FIB       |     49152   |         6    |     49146
|        | IN-V6 ACL       |         0   |         0    |         0
|        | IN-NLB ACL      |         0   |         0    |         0
|        | IPMAC ACL       |         0   |         0    |         0
|        | OUT-L2 ACL      |       206   |         9    |       197
|        | OUT-L3 ACL      |       178   |         9    |       169
|        | OUT-V6 ACL      |       178   |         4    |       174
2   |   0    | IN-L2 ACL       |      1536   |         0    |      1536
|        | IN-L3 ACL       |      1024   |         1    |      1023
|        | IN-L3 FIB       |     49152   |         6    |     49146
|        | IN-V6 ACL       |         0   |         0    |         0
|        | IN-NLB ACL      |         0   |         0    |         0
|        | IPMAC ACL       |         0   |         0    |         0
|        | OUT-L2 ACL      |       206   |         9    |       197
|        | OUT-L3 ACL      |       178   |         9    |       169
|        | OUT-V6 ACL      |       178   |         4    |       174
3   |   0    | IN-L2 ACL       |      1536   |         0    |      1536
|        | IN-L3 ACL       |      1024   |         1    |      1023
|        | IN-L3 FIB       |     49152   |         6    |     49146
|        | IN-V6 ACL       |         0   |         0    |         0
|        | IN-NLB ACL      |         0   |         0    |         0
|        | IPMAC ACL       |         0   |         0    |         0
|        | OUT-L2 ACL      |       206   |         9    |       197
|        | OUT-L3 ACL      |       178   |         9    |       169
|        | OUT-V6 ACL      |       178   |         4    |       174

Codes: * - cam usage is above 90%.
```

**Example 2:** Output of the `show cam-usage acl` Command

```
Dell#show cam-usage acl
Stackunit|Portpipe| CAM Partition   | Total CAM   |  Used CAM   | Available CAM
========|========|=================|=============|=============|==============
1   |   0    | IN-L2 ACL       |      1536   |         0    |      1536
|        | IN-L3 ACL       |      1024   |         1    |      1023
|        | IN-V6 ACL       |         0   |         0    |         0
|        | OUT-L2 ACL      |       206   |         9    |       197
|        | OUT-L3 ACL      |       178   |         9    |       169
|        | OUT-V6 ACL      |       178   |         4    |       174
2   |   0    | IN-L2 ACL       |      1536   |         0    |      1536
|        | IN-L3 ACL       |      1024   |         1    |      1023
|        | IN-V6 ACL       |         0   |         0    |         0
|        | OUT-L2 ACL      |       206   |         9    |       197
|        | OUT-L3 ACL      |       178   |         9    |       169
|        | OUT-V6 ACL      |       178   |         4    |       174
```

Access Control List (ACL) VLAN Groups and Content Addressable Memory (CAM)
### 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.3.(0.0) | Introduced on the S4810, S4820T, Z9000 and MXL platforms

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
Dell#

**acl-vlan-group**

Create an ACL VLAN group.

**Syntax**

```plaintext
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

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

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.3.(0.0) | Introduced on the S4810, S4820T and Z9000 platforms

**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

**Command History**

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

**Version**

- 9.8(0.0P5)  
  Introduced on the S4048-ON.
- 9.8(0.0P2)  
  Introduced on the S3048-ON.
- 9.3,(0,0)  
  Introduced on the S4810, S4820T, Z9000 and MXL platforms

**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
Dell#
```
**description (ACL VLAN Group)**

Add a description to the ACL VLAN group.

**Syntax**

```plaintext
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)

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3.(0.0)</td>
<td>Introduced on the S4810, S4820T, and Z9000 platforms</td>
</tr>
</tbody>
</table>

**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 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 VLAN interfaces and port-channels.

Topics:
- bfd all-neighbors
- bfd disable
- bfd enable (Configuration)
- bfd enable (Interface)
- bfd interval
- bfd neighbor
- bfd protocol-liveness
- ip route bfd
- 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.

**Syntax**

```
bfd all-neighbors [interval interval min_rx min_rx multiplier value role {active | passive}]
```

**Parameters**

- `interval milliseconds` (OPTIONAL) Enter the keyword interval to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 200.
- `min_rx milliseconds` Enter the keyword min_rx to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is 200.
- `multiplier value` Enter the keyword multiplier to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.
- `role [active | passive]` Enter the role that the local system assumes:
  - Active — The active system initiates the BFD session. Both systems can be active for the same session.
Passive — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is active.

Defaults

See Parameters.

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 Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced BFD for BGP on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced BFD for BGP on the S4810.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>Introduced BFD for BGP on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced BFD for OSPF and ISIS on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced BFD for OSPF on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced BFD for ISIS on the E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced BFD for OSPF on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

All neighbors inherit the timer values configured with the bfd neighbor command except in the following cases:

- Timer values configured with the isis bfd all-neighbors or ip ospf bfd all-neighbors commands in INTERFACE mode override timer values configured with the bfd neighbor command. Likewise, using the no bfd neighbor command does not disable BFD on an interface if you explicitly enable BFD using the isis bfd all-neighbors command.
- Neighbors that have been explicitly enabled or disabled for a BFD session with the bfd neighbor or neighbor bfd disable commands in ROUTER BGP mode do not inherit the global BFD enable/disable values configured with the bfd neighbor command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the bfd neighbor command).

You can only enable BFD for VRRP in INTERFACE command mode (vrrp bfd all-neighbors).
Related Commands

- `neighbor bfd disable` — disable a BFD session explicitly with a BGP neighbor or a BGP peer group.

**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**

VRRP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### 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

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(10.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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**

- `interval milliseconds` Enter the keywords interval to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 200.
- `min_rx milliseconds` Enter the keywords min_rx to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is 200.
- `multiplier value` Enter the keywords multiplier to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.
role [active | passive]

Enter the role that the local system assumes:

- **Active** — The active system initiates the BFD session. Both systems can be active for the same session.
- **Passive** — The passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

**Defaults**
Refer to **Parameters**.

**Command Modes**
INTERFACE

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf-if-gi-1/3)# bfd interval 250 min_rx 300 multiplier 4 role passive
Dell(conf-if-gi-1/3)#
```

### bfd neighbor

Establish a BFD session with a neighbor.

**Syntax**

```
bfd neighbor ip-address
```

To remove the BFD session with the neighbor, use the `no bfd neighbor ip-address` command.

**Parameters**

- **ip-address**
  
Enter the IP address of the neighbor in dotted decimal format (A.B.C.D).

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
Version Description
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.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.10.0 Introduced on the S4810.
8.2.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the C-Series.
7.5.1.0 Added support for VLAN and port-channel interfaces on the E-Series.

Related Commands
• show bfd neighbors — display the BFD neighbor information on all interfaces or a specified interface.

**bfd protocol-liveness**

Enable the BFD protocol liveness feature.

**Syntax**
bfd protocol-liveness

**Defaults**
Disabled

**Command Modes**
CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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 [interval interval min_rx min_rx multiplier value role {active | passive}]
To disable BFD for all neighbors configured through static routes, use the `no ip route bfd [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

**Parameters**

- **interval milliseconds** (OPTIONAL) Enter the keywords **interval** to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
- **min_rx milliseconds** Enter the keywords **min_rx** to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
- **multiplier value** Enter the keywords **multiplier** to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
- **role [active | passive]** Enter the role that the local system assumes:
  - **Active** — active system initiates the BFD session. Both systems can be active for the same session.
  - **Passive** — passive system does not initiate a session. It only responds to a request for session initialization from the active system.

The default is **Active**.

**Defaults**

See Parameters.

**Command Modes**

CONFIGURATION

**Command History**

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

**Version** | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.3.(0.0) | Introduced on S6000.
9.2(1.0) | Introduced on the Z9500.
9.2.(0.0) | Introduced on Z9000, S4810, and S4820T.
8.2.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the C-Series.
7.4.1.0 | Introduced on the E-Series.

**ipv6 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 in interface mode.

**Parameters**

- **disable**  
  (OPTIONAL) Enter the keyword *disable* to disable BFD on this interface.

- **interval milliseconds**  
  (OPTIONAL) Enter the keyword *interval* to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 200.

- **min_rx milliseconds**  
  Enter the keywords *min_rx* to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is 200.

- **multiplier value**  
  Enter the keyword *multiplier* to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.

- **role [active | passive]**  
  Enter the role that the local system assumes:
  - **Active** — active system initiates the BFD session. Both systems can be active for the same session.
  - **Passive** — passive system does not initiate a session. It only responds to a request for session initialization from the active system.

  The default is **Active**.

**Defaults**  
See Parameters.

**Command Modes**  
INTERFACE

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

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2.0.0 | Introduced on the Z9000, S4820T, and S4810.

**Usage Information**  
This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure ipv6 ospf BFD in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the bfd all-neighbors command. Using the no form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword *disable*.

### 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>(OPTIONAL) Enter the keyword <code>disable</code> to disable BFD on this interface.</td>
</tr>
<tr>
<td>interval milliseconds</td>
<td>(OPTIONAL) Enter the keywords <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 200.</td>
</tr>
<tr>
<td>min_rx milliseconds</td>
<td>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 200.</td>
</tr>
<tr>
<td>multiplier value</td>
<td>Enter the keywords <code>multiplier</code> to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.</td>
</tr>
<tr>
<td>role [active</td>
<td>passive]</td>
</tr>
<tr>
<td></td>
<td>• Active — active system initiates the BFD session. Both systems can be active for the same session.</td>
</tr>
<tr>
<td></td>
<td>• Passive — passive system does not initiate a session. It only responds to a request for session initialization from the active system.</td>
</tr>
</tbody>
</table>

The default is **Active**.

### Defaults

See **Parameters**.

### Command Modes

**INTERFACE**

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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

ROUTE BG

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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` — disable a BFD session explicitly with a BGP neighbor or a BGP peer group.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

Syntax

```
neighbor {ip-address | peer-group-name} bfd disable
```
**Parameters**

- **ip-address**
  Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).

- **peer-group-name**
  Enter the name of the peer group that you want to explicitly disable for BFD sessions.

**Defaults**

None

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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 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.

When you remove the Disabled state of a BFD for a BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd neighbor` command or configured for the peer group to which the neighbor belongs.

**Related Commands**

- **neighbor bfd** — enable a BFD session explicitly with a BGP neighbor or a BGP peer group.

### show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

**Syntax**

```
show bfd neighbors [interface [detail]]
```

**Parameters**

- **interface**
  Enter one of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
• For a 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 Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Added support for BFD for BGP on the S4810.</td>
</tr>
<tr>
<td>8.4.1.3</td>
<td>Added support for BFD for BGP on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for BFD for VLAN and port-channel interfaces on the E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced BFD on physical ports on the E-Series.</td>
</tr>
</tbody>
</table>

Example  Dell# show bfd neighbors

*       - Active session role
Ad Dn   - Admin Down
B       - BGP
C       - CLI
I       - ISIS
O       - OSPF
O3      - OSPFv3
R       - Static Route (RTM)

LocalAddr  RemoteAddr  Interface State Rx-int Tx-int Mult Clients
* 10.1.3.2  10.1.3.1   Gi 1/3    Up   300   250   3  C

Example (Detail)  Dell# show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: GigabitEthernet 1/3
State: Up
Configured parameters:
TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
  TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
  TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
  Number of packets received from neighbor: 376
  Number of packets sent to neighbor: 314
  Number of state changes: 2
  Number of messages from IFA about port state change: 0
  Number of messages communicated b/w Manager and Agent: 6

vrrp bfd neighbor

Establish a BFD for VRRP session with a neighbor.

Syntax
vrrp bfd neighbor ip-address

To remove the BFD session with the neighbor, use the no vrrp bfd neighbor ip-address command.

Parameters
  ip-address Enter the IP address of the neighbor in dotted decimal format (A,B,C,D).

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for VLAN and port-channel interfaces on the E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands
  - bfd all-neighbors — establish BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.
  - show bfd neighbors — display the BFD neighbor information on all interfaces or a specified interface.
BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless inter-domain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically sent messages to update those routing tables.

NOTE: For more information about configuring the border gateway protocol (BGP), see the BGP section in the Dell Networking OS Configuration Guide.

Topics:
- BGP IPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)
- IPv6 BGP Commands
- IPv6 MBGP Commands

### BGP IPv4 Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP supports classless interdomain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

NOTE: Dell Networking OS supports 2-byte (16-bit) and 4-byte (32-bit) format for autonomous system numbers (ASNs), where the 2-byte format is 1 to 65535 and the 4-byte format is 1 to 4294967295.

NOTE: Dell Networking OS supports dotted format as well as the traditional plain format for AS numbers. The dot format is displayed when using the show ip bgp commands. To determine the comparable dot format for an ASN from a traditional format, use ASN/65536. ASN%65536. For more information about using the 2- or 4-byte format, refer to the Dell Networking OS Configuration Guide.

**address-family**

Enable the IPv4 multicast or the IPv6 address family.

**Syntax**

```
address-family {ipv4 {multicast [vrf vrf-name]} | ipv6 unicast [vrf vrf-name]}
```

**Parameters**

- **ipv4 multicast**
  Enter the keyword ipv4 followed by the keyword multicast to enable BGPv4 multicast mode.

- **ipv4 vrf vrf-name**
  Enter the keyword ipv4 followed by the keyword vrf and then the name of the VRF to enable VRF mode.
NOTE: Use this attribute to start a BGP instance corresponding to either a specific address family in a default VRF or an IPv4 address family in a non-default VRF.

ipv6 unicast

Enter the keyword ipv6 followed by the keyword unicast to enable BGPv6 mode.

vrf vrf-name

(Optional) Enter the keyword vrf followed by the name of the VRF to install the IPv6 route in that VRF.

NOTE: It will not be possible to enable VRF mode for IPv6 unicast without configuring the corresponding IPv4 unicast mode for the same VRF. While deletion, whenever the IPv4 VRF mode is deleted for the VRF, it will automatically delete the IPv6 VRF configurations as well.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

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

Version Description

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

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Added support for IPv6 VRF.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

6.5.1.0 Introduced

aggregate-address

To minimize the number of entries in the routing table, summarize a range of prefixes.

Syntax

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

Parameters

ip-address mask Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).

advertise-map map-name (OPTIONAL) Enter the keywords advertise-map then the name of a configured route map to set filters for advertising an aggregate route.

as-set (OPTIONAL) Enter the keyword as-set to generate path attribute information and include it in the aggregate.
AS_SET includes AS_PATH and community information from the routes included in the aggregated route.

**attribute-map map-name**  (OPTIONAL) Enter the keywords attribute-map then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.

**summary-only**  (OPTIONAL) Enter the keyword summary-only to advertise only the aggregate address. Specific routes are not advertised.

**suppress-map map-name**  (OPTIONAL) Enter the keywords suppress-map then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

**Defaults**
Not configured.

**Command Modes**
- ROUTER BGP ADDRESS FAMILY
- ROUTER BGP ADDRESS FAMILY IPv6

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the as-set parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the suppress-map parameter, routes meeting the deny clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the permit clause are suppressed.

If the route is injected via the network command, that route still appears in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

In the show ip bgp command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.
When an aggregate address is denied using a peer’s outbound route-map, individual routes suppressed by the aggregate address are advertised to that peer.

The attribute-map corresponding to an aggregate address is applied during the outbound update creation time; the value set in that attribute-map will not be shown in the output of the `show ip bgp aggregate route` command.

**bgp add-path**

Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

**Syntax**

```
bgp add-path [send | receive | both] path-count
```

**Parameters**

- **send**
  - Enter the keyword `send` to indicate that the system sends multiple paths to peers.
- **receive**
  - Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
- **both**
  - Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
- **path-count**
  - Enter the number paths supported. The range is from 2 to 64.

**Defaults**

Disabled

**Command Modes**

- ROUTER BGP
- ROUTER BGP-address-family

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `neighbor add-path` — specify that this neighbor/peer group can send/receive multiple path advertisements.
bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax
bgp always-compare-med
To disable comparison of MED, enter no bgp always-compare-med.

Defaults
Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced command.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
Any update without a MED attribute is the least preferred route.

If you enable this command, use the clear ip bgp * command to recompute the best path.

bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

Syntax
bgp asnotation [asplain | asdot+ | asdot]
To disable a dot or dot+ representation and return to ASPLAIN, enter the no bgp asnotation command.

Defaults
asplain

Command Modes
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced the dynamic application of AS notation changes.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

Before enabling this feature, enable the `enable bgp four-octet-as-support` command. If you disable the `four-octect-support` command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation shows.

**Example**

```
Dell(conf)# router bgp 1
Dell(conf-router_bgp)# bgp asnotation asdot
Dell(conf-router_bgp)# ex
Dell(conf)# do show run | grep bgp

router bgp 1  
  bgp four-octet-as-support  
  bgp asnotation asdot

Dell(conf)# router bgp 1
Dell(conf-router_bgp)# bgp asnotation asdot+
Dell(conf-router_bgp)# ex

Dell(conf)# do show run | grep bgp
router bgp 1  
  bgp four-octet-as-support  
  bgp asnotation asdot+

Dell(conf)# router bgp 1
Dell(conf-router_bgp)# bgp asnotation asplain
Dell(conf-router_bgp)# ex
Dell(conf)# do show run | grep bgp
router bgp 1  
  bgp four-octet-as-support

Dell(conf)#
```

**Related Commands**

- `bgp four-octet-as-support` — enable 4-byte support for the BGP process.

**bgp bestpath as-path ignore**

Ignore the AS PATH in BGP best path calculations.

**Syntax**

```
bgp bestpath as-path ignore
```

To return to the default, enter the `no bgp bestpath as-path ignore` command.
Defaults
Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
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

**Command History**

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

**Version**

- **9.8(0.0P5)**
  Introduced on the S4048-ON.
- **9.8(0.0P2)**
  Introduced on the S3048-ON.
- **9.7(0.0)**
  Introduced on the S6000--ON.
- **9.2(1.0)**
  Introduced on the Z9500.
- **9.0.2.0**
  Introduced on the S6000.
- **8.3.19.0**
  Introduced on the S4820T.
- **8.3.11.1**
  Introduced on the Z9000.
- **8.3.7.0**
  Introduced on the S4810.
- **7.8.1.0**
  Introduced on the S-Series.
- **7.7.1.0**
  Introduced on the C-Series.

**Usage Information**

The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

**bgp bestpath med missing-as-best**

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over paths with an advertised MED attribute.

**Syntax**

```
bgp bestpath med missing-as-best
```

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

**Defaults**

Disabled

**Command Modes**

ROUTER BGP
Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over paths with a higher MED.

**bgp bestpath router-id ignore**

Do not compare router-id information for external paths during best path selection.

**Syntax**

```
bgp bestpath router-id ignore
```

To return to the default selection, use the `no bgp bestpath router-id ignore` command.

**Defaults**

Disabled

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Usage Information
Configuring this option retains the current best-path. When sessions are then reset, the oldest received path is chosen as the best-path.

**bgp client-to-client reflection**

Allows you to enable route reflection between clients in a cluster.

**Syntax**

```
bgp client-to-client reflection
```

To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.

**Defaults**

Enabled when a route reflector is configured.

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Route reflection to clients is not necessary if all client routers are fully meshed.

**Related Commands**

- `bgp cluster-id` — assign an ID to a BGP cluster with two or more route reflectors.
- `neighbor route-reflector-client` — configure 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}
```

**Usage Information**

Route reflection to clients is not necessary if all client routers are fully meshed.
To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

### Parameters
- **ip-address**
Enter an IP address as the route reflector cluster ID.
- **number**
Enter a route reflector cluster ID as a number from 1 to 4294967295.

### Defaults
Not configured.

### Command Modes
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### Usage Information
When a BGP cluster contains only one route reflector, the cluster ID is the route reflector’s router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

This command automatically restarts the BGP instance for the configuration to take effect.

### Related Commands
- `bgp client-to-client reflection` — enable route reflection between the route reflector and clients.
- `neighbor route-reflector-client` — configure a route reflector and clients.
- `show ip bgp cluster-list` — view paths with a cluster ID.

---

**bgp confederation identifier**

Configure an identifier for a BGP confederation.

### Syntax
```
bgp confederation identifier as-number
```
To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.
Parameters

as-number Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

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

Version Description

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

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000–ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

7.8.1.0 Introduced on the S-Series.

7.7.1.0 Introduced on the C-Series. Added support for the 4-byte format

Usage Information

To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

Dell Networking OS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

If a local-as is configured, BGP does not allow for the configuration of BGP confederation. Similarly, if BGP confederation is configured, then BGP does not allow the configuration of local-as.

If the neighbor is an eBGP neighbor, then BGP performs a check on the first AS number. In this scenario, it is mandatory that the first sequence in the AS path is of type AS_SEQUENCE or AS_CONFED_SEQUENCE (in the case of confederations). If the first entry appears as an AS_CONFED_SET and the neighbor is not in the local AS, then this is strictly a problem with the neighbor node.

This command automatically restarts the BGP instance for the configuration to take effect.

Related Commands

- bgp four-octet-as-support — enable 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

- `as-number` Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).
- `...as-number` (OPTIONAL) Enter up to 16 confederation numbers. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.  Added support for the 4-byte format.</td>
</tr>
</tbody>
</table>

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` — configure a confederation ID.
- `bgp four-octet-as-support` — enable 4-byte support for the BGP process.
### bgp connection-retry-timer

Configures the BGP connection retry timer.

**Syntax**

```
bgp connection-retry-timer retry-timer-value
```

To return to the default configuration, enter the `no connection-retry-timer retry-timer-value` command.

**Parameters**

- `retry-timer-value` Enter a value that denotes the time interval after which the session retries the connection. The valid range is from 10 to 65535.

**Defaults**

60 seconds.

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### 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**

- `half-life` (OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.

- `reuse` (OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route’s Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is **750**.

- `suppress` (OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route’s Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is **2000**.

- `max-suppress-time` (OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is **60 minutes**.
route-map map-name

(Optional) Enter the keyword route-map then the name of a configured route map.

Only match commands in the configured route map are supported.

**Defaults**

Disabled.

**Command Modes**

- ROUTER BGP
- ROUTER BGP-address-family

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you enter the bgp dampening command, the default values for half-life, reuse, suppress, and max-suppress-time are applied. The parameters are position-dependent; therefore, if you configure one parameter, configure the parameters in the order they appear in the CLI.

Route refresh is sent when you enable BGP dampening.

**Related Commands**

- show ip bgp dampened-paths — view 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
**bgp dmzlink-bw**

Enables BGP Link Bandwidth.

**Syntax**

```
bgp dmzlink-bw
```

To disable BGP Link Bandwidth, enter the `no bgp dmzlink-bw` command.

**Parameters**

- `dmzlink-bw`: Enter the keyword `dmzlink-bw` to enable BGP Link Bandwidth in BGP multipath.

**Defaults**

N/A

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

All routers apply the `bgp default local-preference` command setting within the AS. To set the local preference for a specific route, use the `set local-preference` command in ROUTE-MAP mode.
Version  Description
9.2(1.0)  Introduced on the Z9500.

Usage Information
Configuring or un-configuring the command brings down and brings up the BGP Route Manager, this results in tear down and re-establishment of all active sessions.

Link Bandwidth has to be configured on the router to tell it to associate Link Bandwidth with prefixes (paths) and/or to use Link Bandwidth in BGP Multipath route selection.

This is done under BGP configuration and is supported per address family – for IPv4 and IPv6 address families.

The configuration for a particular address family applies across all VRFs configured.

This command must be performed on the router which is attaching link bandwidth to prefixes (typically a border router) as well as the router which is expected to load share traffic proportional to the bandwidth of the external links.

### bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

**Syntax**

```
bgp enforce-first-as
```

To turn off the default, use the `no bgp enforce-first-as` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is increments. Use the `show ip bgp neighbors` command to view the “failed enforce-first-as check” counter.

If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.
In the event of an enforce-first-as check failure, the existing BGP session is flapped.

Related Commands

- `show ip bgp neighbors` — view the information the BGP neighbors exchange.
- `show ip protocols` — view 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.

**Defaults**

Enabled

**Command Modes**

- `ROUTER BGP`

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

- The `bgp fast-external-fallover` command appears in the `show config` command output.

The fast external fallover configuration is applied only after you manually reset all the existing BGP sessions. As a result, after you execute this command, you must also manually execute the `clear ip bgp` command in order for the configuration to take effect.
**bgp four-octet-as-support**

Enable 4-byte support for the BGP process.

**Syntax**

```plaintext
bgp four-octet-as-support
To disable fast external failover, use the no bgp four-octet-as-support command.
```

**Defaults**

Disabled (supports 2-byte format)

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.71.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router.

When creating Confederations, all the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

Where the 2-byte format is from 1 to 65535, the 4-byte format is from 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format.

For more information about using the 2 byte or 4-byte format, refer to the Dell Networking OS Configuration Guide.

This command automatically restarts the BGP instance for the configuration to take effect.

---

**bgp graceful-restart**

To support graceful restart as a receiver only, enable graceful restart on a BGP neighbor, a BGP node, or designate a local router.

**Syntax**

```plaintext
bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]
```

**Usage Information**

Conformant BGP speakers cannot communicate with non-conformant BGP speakers.

When a router is configured to support graceful restart, it can issue a restart request to its peers. A peer that receives the request acknowledges it or sends a reject message. If the router does not receive an acknowledgement, it sends a grace period number of messages to its peer before assuming the peer will not support graceful restart.

By default, the router is configured to support both roles (i.e., receiver and transmitter) of graceful restart.

The graceful restart process is initiated by the router if:

1. The router is the destination of a restart request.
2. The router is the neighbor of a restarting router.
3. The router is the neighbor of a router that has received a notification that a router is restarting.

Graceful restart begins when a router receives a restart request for a router that is not a successor router. The router sends a message to the source of the request and sets a restart timer. When the restart timer expires, the router sends a restart acknowledge message to the source of the request.

The graceful restart process is not compatible with some BGP versions.

The graceful restart process is initiated by the router if:

1. The router is the destination of a restart request.
2. The router is the neighbor of a restarting router.
3. The router is the neighbor of a router that has received a notification that a router is restarting.

Graceful restart begins when a router receives a restart request for a router that is not a successor router. The router sends a message to the source of the request and sets a restart timer. When the restart timer expires, the router sends a restart acknowledge message to the source of the request.

The graceful restart process is not compatible with some BGP versions.

This command automatically restarts the BGP instance for the configuration to take effect.
To return to the default, use the `no bgp graceful-restart` command.

**Parameters**

- **restart-time seconds** Enter the keyword `restart-time` then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is **120 seconds**.
- **stale-path-time seconds** Enter the keyword `stale-path-time` then the maximum number of seconds to wait before restarting a peer’s stale paths. The default is **360 seconds**.
- **role receiver-only** Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

**Defaults**

As above

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

This command automatically restarts the BGP instance for the configuration to take effect.

**bgp non-deterministic-med**

Compare MEDs of paths from different autonomous systems.

**Syntax**

```
bgp non-deterministic-med
```

To return to the default, use the `no bgp non-deterministic-med` command.

**Defaults**

Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).

**Command Modes**

ROUTER BGP
### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to Dell Networking OS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (no bgp non-deterministic-med), Dell Networking OS compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

### bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

**Syntax**

```
bgp recursive-bgp-next-hop
```

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

**Defaults**

Enabled

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
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 — clear 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)

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.
7.7.1.0 Introduced on the C-Series.
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 expense 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 51 Routing for Networks
    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-failover 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` — view information on all routing protocols enabled and active on the E-Series.

### bgp router-id

Assign a user-given ID to a BGP router.

**Syntax**

```
bgp router-id ip-address
```

To delete a user-assigned IP address, use the `no bgp router-id` command.

**Parameters**

- `ip-address` Enter an IP address in dotted decimal format to reset only that BGP neighbor.

**Defaults**

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

**Command Modes**

- `ROUTER BGP`

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Peering sessions are reset when you change the router ID of a BGP router.

This command automatically restarts the BGP instance for the configuration to take effect.

**clear ip bgp**

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

**Syntax**

```
clear ip bgp [vrf vrf-name] [* | <1-4294967295> | <0.1-65535.65535> | A.B.C.D
{soft {in | out}} | X:X:X::X {soft {in | out}}] dampening flap-statistics
ipv4 | ipv6 | peer-group]
```

**Parameters**

- `vrf vrf-name` Enter the keyword vrf and then the name of the VRF to clear all BGP sessions corresponding to that VRF.
  
  **NOTE:** Use this attribute to clear a BGP instance corresponding to either a specific address family in a default VRF or an IPv4 address family in a non-default VRF.

- `*` Enter an asterisk (*) to reset all BGP sessions.

- `<1-4294967295>` Enter <1-4294967295> to clear peers with the AS number.

- `<0.1-65535.65535>` Enter <0.1-65535.65535> to clear peers with the AS number in dot format.

- `A.B.C.D` Enter the BGP neighbor address in the A.B.C.D format to clear.

- `X:X:X::X` Enter the BGP neighbor address in the X:X:X::X format to clear.

- `soft` (OPTIONAL) Enter the keyword soft to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.

  **NOTE:** If you enter the clear ip bgp ip-address soft command, both inbound and outbound policies are reset.

- `in` (OPTIONAL) Enter the keyword in to activate only inbound policies.
out (OPTIONAL) Enter the keyword out to activate only outbound policies.

NOTE: You must execute the clear ip bgp soft out command whenever there is a change in the local policy. If you do not run this command after a local policy change, then these policy changes are not reflected in the responses to the peer's route refresh messages.

dampening Enter the keyword dampening to clear the flap dampening information.

flap-statistics Enter the keywords flap-statistics to clear the flap statistics information.

ipv4 Enter the ipv4 address family to clear.

ipv6 Enter the ipv6 address family to clear.

peer-group Enter the peer-group to clear all members of the peer-group.

Command Modes EXEC Privilege

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.
7.7.1.0 Introduced on the C-Series.
6.5.1.0 Expanded to include the as-number option.

Related Commands - bgp recursive-bgp-next-hop — disable next-hop resolution through other routes learned by the BGP.

clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

Syntax clear ip bgp [vrf vrf-name] [ipv4 [multicast | unicast] | ipv6 unicast] [dampening [ipv4-address mask | ipv6-address mask]]

Parameters vrf vrf-name (OPTIONAL) Enter the keyword vrf and then the name of the VRF to clear information on route dampening corresponding to that VRF.
NOTE: You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.

```
ipv4 multicast  (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to clear the ipv4 multicast routes.

ipv4 unicast     (OPTIONAL) Enter the keyword ipv4 followed by the keyword unicast to clear the ipv4 unicast routes.

ipv6 unicast     (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to clear the ipv6 unicast routes.

ipv4-address mask (OPTIONAL) Enter an IPv4 address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

ipv6-address mask (OPTIONAL) Enter the IPv6 address and the network mask to clear information on IPv6 route dampening.
```

**Command Modes**

EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Added the ipv4 multicast and ipv6 unicast parameters.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.

**Usage Information**

After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.

The **clear ip bgp dampening** command does not clear the history paths.
clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax

```
clear ip bgp [vrf vrf-name] [ipv4 [multicast | unicast] | ipv6 unicast] [flap-statistics [ipv4-address mask | ipv6-address mask] | filter-list as-path-name | regexp regular-expression]
```

Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf and then the name of the VRF to clear BGP flap statistics corresponding to that VRF.
  - **NOTE:** You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.

- **ipv4 multicast** (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to clear information related only to ipv4 multicast routes.

- **ipv4 unicast** (OPTIONAL) Enter the keyword ipv4 followed by the keyword unicast to clear information related only to ipv4 unicast routes.

- **ipv6 unicast** (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to clear information related only to ipv6 unicast routes.

- **ipv4-address mask** (OPTIONAL) Enter an IPv4 address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.

- **ipv6-address mask** (OPTIONAL) Enter the IPv6 address followed by the network mask to reset only that prefix.

- **filter-list as-path-name** (OPTIONAL) Enter the keywords filter-list then the name of a configured AS-PATH list.

- **regexp regular-expression** (OPTIONAL) Enter the keyword regexp then regular expressions. Use one or a combination of the following:
  - . = (period) any single character (including a white space).
  - * = (asterisk) the sequences in a pattern (0 or more sequences).
  - + = (plus) the sequences in a pattern (1 or more sequences).
  - ? = (question mark) sequences in a pattern (either 0 or 1 sequences).
  - ^ = (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.

- **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.

Command Modes

EXEC Privilege
Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the ipv4 multicast and ipv6 unicast parameters.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If you enter the `clear ip bgp flap-statistics` command without any parameters, all statistics are cleared.

Related Commands

- `show debugging` — view the enabled debugging operations.
- `show ip bgp flap-statistics` — view the BGP flap statistics.
- `undebug all` — disable all debugging operations.

**clear ip bgp peer-group**

Reset a peer-group’s BGP sessions.

**Syntax**

```
clear ip bgp [vrf vrf-name] peer-group peer-group-name [ipv4 [multicast | unicast] | ipv6 unicast] [soft {in | out}]
```

**Parameters**

- `vrf vrf-name`  
Enter the keyword `vrf` and then the name of the VRF to reset the peer group corresponding to that VRF.
  
  ***NOTE:*** You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.

- `peer-group-name`  
Enter the peer group name to reset the BGP sessions within that peer group.

- `ipv4 multicast`  
  (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to reset ipv4 multicast routes.

- `ipv4 unicast`  
  (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to reset ipv4 unicast routes.
deny bandwidth

Enables you to specify link band width extended-community attribute as the matching criteria to deny incoming or outgoing traffic.

Syntax

```
deny bandwidth
```

To disable this setting, enter the `no deny bandwidth` command.

Parameters

- **bandwidth**: Enter the keyword `bandwidth` to specify extended-community attribute as the matching criteria for denying traffic. The range is from 0 to 102400.

Defaults

N/A

Command Modes

EXTENDED COMMUNITY LIST

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the ipv4 multicast and ipv6 unicast parameters.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax
deb ug ip bgp [ vrf vrf-name | A.B.C.D | X:X:X:X::X | peer-group peer-group-name] [in | out]
To disable all BGP debugging, use the no debug ip bgp command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>Enter the keyword vrf and then the name of the VRF to debug BGP information corresponding to that VRF.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>Enter the IPv4 address of the neighbor in dotted decimal format.</td>
</tr>
<tr>
<td>X:X:X:X:X</td>
<td>(OPTIONAL) Enter an IPv6 address.</td>
</tr>
<tr>
<td>peer-group peer-group-name</td>
<td>Enter the keywords peer-group then the name of the peer group to debug.</td>
</tr>
<tr>
<td>in</td>
<td>(OPTIONAL) Enter the keyword in to view only information on inbound BGP routes.</td>
</tr>
<tr>
<td>out</td>
<td>(OPTIONAL) Enter the keyword out to view only information on outbound BGP routes.</td>
</tr>
<tr>
<td>ipv4 ipv6</td>
<td>Enter the IPv4 address to view the IPV4 route information.</td>
</tr>
<tr>
<td>keepalives</td>
<td>Enter the keyword keepalives to view BGP keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Enter the keyword notifications to view BGP notifications.</td>
</tr>
<tr>
<td>dampening</td>
<td>Enter the keyword dampening to view BGP dampening.</td>
</tr>
<tr>
<td>events</td>
<td>Enter the keyword events to view BGP protocol events.</td>
</tr>
<tr>
<td>ipv4 ipv6</td>
<td>Enter the IPv4 IP address to view the IPV4 route information.</td>
</tr>
<tr>
<td>keepalives</td>
<td>Enter the keyword keepalives to view BGP keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Enter the keyword notifications to view BGP notifications.</td>
</tr>
<tr>
<td>soft-reconfiguration</td>
<td>Enter the keywords soft-reconfiguration to view only information on inbound BGP soft reconfiguration.</td>
</tr>
<tr>
<td>updates</td>
<td>Enter the keyword updates to view BGP updates.</td>
</tr>
</tbody>
</table>

Command Modes EXEC Privilege
**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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` — view information about BGP events.
- `debug ip bgp keepalives` — view information about BGP keepalives.
- `debug ip bgp notifications` — view information about BGP notifications.
- `debug ip bgp updates` — view information about BGP updates.
- `show debugging` — view enabled debugging operations.

### debug ip bgp dampening

View information on routes being dampened.

**Syntax**

debug ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 unicast] dampening

To disable debugging, use the `no debug ip bgp dampening` command.

**Parameters**

- **vrf vrf-name**
  
Enter the keyword `vrf` followed by the name of the VRF to view information on dampened routes corresponding to that VRF.

- **ipv4 multicast**
  
  (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view dampened-route information related only to ipv4 multicast routes.

- **ipv4 unicast**
  
  (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view dampened-route information related only to ipv4 unicast routes.
Optional) Enter the keyword ipv4 followed by the keyword unicast to view dampened-route information related only to ipv6 unicast routes.

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for the E-Series.</td>
</tr>
</tbody>
</table>

### debug ip bgp events

Display information on local BGP state changes and other BGP events.

**Syntax**

ddebug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group peer-group-name] events [in | out]

To disable debugging, use the no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group peer-group-name] events [in | out] command.

**Parameters**

- **vrf vrf-name**  
  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display BGP state changes corresponding to that VRF.

- **A.B.C.D**  
  (OPTIONAL) Enter the IPv4 address of the neighbor.

- **X:X:X::X**  
  (OPTIONAL) Enter an IPv6 address.

- **peer-group peer-group-name**  
  (OPTIONAL) Enter the keyword peer-group then the name of the peer group.

- **in**  
  (OPTIONAL) Enter the keyword in to view only events on inbound BGP messages.

- **out**  
  (OPTIONAL) Enter the keyword out to view only events on outbound BGP messages.
**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

**debug ip bgp keepalives**

Display information about BGP keepalive messages.

**Syntax**

debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] keepalives [in | out]

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] keepalives [in | out]` command.

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display BGP keepalive information corresponding to that VRF.
- **A.B.C.D** (OPTIONAL) Enter the IPv4 address of the neighbor.
- **X:X:X:X::X** (OPTIONAL) Enter an IPv6 address.
- **peer-group peer-group-name** (OPTIONAL) Enter the keyword peer-group then the name of the peer group.
- **in** (OPTIONAL) Enter the keyword in to view only inbound keepalive messages.
- **out** (OPTIONAL) Enter the keyword out to view only outbound keepalive messages.

**Command Modes**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

**debug ip bgp notifications**

Allows you to view information about BGP notifications received from neighbors.

**Syntax**

```
debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X] [peer-group peer-group-name] notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X] [peer-group peer-group-name] notifications [in | out]` command.

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to view neighbor BGP notification information corresponding to that VRF.
- `A.B.C.D` (OPTIONAL) Enter the IPv4 address of the neighbor.
- `X:X:X:X::X` (OPTIONAL) Enter an IPv6 address.
- `peer-group peer-group-name` (OPTIONAL) Enter the keyword peer-group then the name of the peer group.
- `in` (OPTIONAL) Enter the keyword in to view BGP notifications received from neighbors.
- `out` (OPTIONAL) Enter the keyword out to view BGP notifications sent to neighbors.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

**debug ip bgp soft-reconfiguration**

Enable soft-reconfiguration debug.

```
Syntax:
debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group-name] soft-reconfiguration
To disable, use the debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group-name] soft-reconfiguration command.
```

**Parameters**

- **vrf vrf-name**  
  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable soft-reconfiguration debugging on that VRF.
- **A.B.C.D**  
  (OPTIONAL) Enter the IPv4 address of the neighbor in dotted decimal format.
- **X:X:X::X**  
  (OPTIONAL) Enter an IPv6 address.
- **peer-group-name**  
  (OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

**Defaults**

Disabled

**Command Modes**

EXEC Privilege

**Command History**

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

**Version**

- 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.
- 9.0.2.0  
  Introduced on the S6000.
Version | Description
--------|---------------------------------------------------
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0  | Introduced on the S4810.
7.8.1.0  | Introduced on the S-Series.
7.7.1.0  | Introduced on the C-Series.
7.2.1.0  | Introduced.

Usage Information
This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug turns on for all neighbors.

**debug ip bgp updates**

Allows you to view information about BGP updates.

**Syntax**

debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group peer-group-name] updates [in | out | prefix-list prefix-list-name]

To disable debugging, use the no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X::X | peer-group peer-group-name] updates [in | out | prefix-list prefix-list-name] command.

**Parameters**

- **vrf vrf-name**: (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to view BGP updates information corresponding to that VRF.
- **A.B.C.D**: (OPTIONAL) Enter an IPv4 address of the neighbor.
- **X:X:X::X**: (OPTIONAL) Enter an IPv6 address.
- **peer-group peer-group-name**: (OPTIONAL) Enter the keyword peer-group followed by the name of the peer group.
- **in**: (OPTIONAL) Enter the keyword in to view only BGP updates received from neighbors.
- **out**: (OPTIONAL) Enter the keyword out to view only BGP updates sent to neighbors.
- **prefix-list prefix-list-name**: (OPTIONAL) Enter the keyword prefix-list then the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
- **ip-address**: (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: (OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

**Command Modes**
EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

**default-metric**

Allows you to change the metric of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

**Syntax**

```
default-metric number
```

To return to the default setting, use the `no default-metric` command.

**Parameters**

- `number` Enter a number as the metric to be assigned to routes from other protocols. The range is from 1 to 4294967295.

**Defaults**

0

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
**Version** | **Description**
--- | ---
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.

**Usage Information**
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` — enable comparison of all BGP MED attributes.
- `redistribute` — redistribute 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

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.
pre-7.7.1.0 | Introduced.
maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax

```
maximum-paths {ebgp | ibgp} number
```

To return to the default values, enter the `no maximum-paths` command.

Parameters

- **ebgp**
  - Enter the keyword `ebgp` to enable multipath support for External BGP routes.
- **ibgp**
  - Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
- **number**
  - Enter a number as the maximum number of parallel paths. The range is from 2 to 64.

Defaults

None

Command Modes

- `ROUTER BGP`

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Support from 2 to 64 paths on the S4810. Command syntax changed to <code>max-path</code> (was <code>maximum-paths</code>).</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

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

```plaintext
neighbor [ip-address | peer-group-name] activate
```

To disable, use the no neighbor [ip-address | peer-group-name] activate command.

Parameters

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name** (OPTIONAL) Enter the name of the peer group.
- **activate** Enter the keyword activate to enable the neighbor/peer group in the new AFI/SAFI.

Defaults

Disabled

Command Modes

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/Unicast AFI/SAFI. When you use activate in the new context, the neighbor/peer group enables for AFI/SAFI. It is not possible to de-activate a peer from the IPv4 unicast address family.

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

Syntax

```plaintext
neighbor [ip-address | peer-group-name] add-path [send | receive | both] path-count
```

Parameters

- **ip-address** (OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name
(Optional) Enter the name of the peer group.

send
Enter the keyword send to indicate that the system sends multiple paths to peers.

receive
Enter the keyword receive to indicate that the system accepts multiple paths from peers.

both
Enter the keyword both to indicate that the system sends and accepts multiple paths from peers.

path-count
Enter the number paths supported. The range is from 2 to 64.

Defaults
none

Command Modes
CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

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

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.8.0 Introduced on the S4810.

Related Commands
• bgp add-path — allow 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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
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`

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
You cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.

Related Commands

- `bgp four-octet-as-support` — enable 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

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

When you configure a route-map for a BGP peer or peer group with the `neighbor default-originate` command, the command checks for the existence of the route in BGP RIB.

Route-map configuration on a BGP peer or peer group works only when the LOC-RIB contains at least one route.
When you apply a default route to a BGP peer or peer group using the `neighbor default-originate` command, changes to the configured default route-map are applied to the BGP peer or peer group only after a delay of 15 seconds. As a result, you must wait for a period of 15 seconds before manually resetting BGP using the `clear ip bgp` command.

In case of eBGP, the `neighbor default-originate` command does not support `extended-community` as a non-transtive route-map attribute.

You cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.

In order that settings corresponding to the `neighbor default-originate` command take effect, you must execute the `clear ip bgp` command immediately after you execute the `neighbor default-originate` command.

### neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

**Syntax**

```
neighbor {ip-address | peer-group-name} description text
```

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group.
- `text` Enter a continuous text string up to 80 characters.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
**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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

**Related Commands**
- `neighbor route-map` — assign a route map to a neighbor or peer group.
neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax

neighbor \{ ip-address | peer-group-name \} ebgp-multihop \[ ttl \]

To disallow and disconnect connections, use the no neighbor \{ ip-address | peer-group-name \}
ebgp-multihop command.

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group.
- **ttl**: (OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is from 1 to 255. The default is 255.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To prevent loops, the neighbor ebgp-multihop command does not install the default routes of the multihop peer. Networks not directly connected are not considered valid for best-path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

Syntax

neighbor \{ ipv4-address | peer-group-name \} fall-over
To disable, use the no neighbor {ipv4-address | peer-group-name} fall-over command.

Parameters

- **ipv4-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S3048–ON and S4048–ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

When you enable failover, BGP keeps track of IP or IPv6 ability to reach the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for the peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

- show ip bgp neighbors — display information on the BGP neighbors.

neighbor local-as

To accept external routes from neighbors with a local AS number in the AS number path, configure Internal BGP (IBGP) routers.

Syntax

```
neighbor {ip-address | peer-group-name} local-as as-number [no-prepend]
```

To return to the default value, use the no neighbor {ip-address | peer-group-name} local-as command.

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
- **as-number**: Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte) or from 0.1 to 65535.65535 (dotted format).
no prepend

Specifies that local AS values do not prepend to announcements from the neighbor.

Defaults
Not configured.

Command Modes
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
If a local-as is configured, BGP does not allow for the configuration of BGP confederation. Similarly, if BGP confederation is configured, then BGP does not allow the configuration of local-as.

This command automatically restarts the neighbor session for the configuration to take effect.

Related Commands
- `bgp four-octet-as-support` — enable 4-byte support for the BGP process.

**neighbor maximum-prefix**

Control the number of network prefixes received.

Syntax

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]
```

To return to the default values, use the `no neighbor {ip-address | peer-group-name} maximum-prefix maximum` command.

Parameters

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group.
- `maximum` Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
- `threshold` (OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the E-Series software sends a message. The range is from 1 to 100 percent. The default is 75.
warning-only

(OptionalAL) 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.

NOTE: When you set this option, the router accepts BGP prefixes only until the maximum configured value. After the maximum number is reached, the router drops any additional prefixes that it receives.

Defaults

threshold = 75

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If you configure the neighbor maximum-prefix command and the neighbor receives more prefixes than the neighbor maximum-prefix command configuration allows, the neighbor goes down and the show ip bgp summary command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the clear ip bgp command for the neighbor or the peer group to which the neighbor belongs or you enter the neighbor shutdown and neighbor no shutdown commands.

Related Commands

- show ip bgp summary — display 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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
This command automatically restarts the neighbor session for the configuration to take effect.

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established. If you specify a BGP peer group by using the 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} dmzlink-bw
```

To delete a peer from a peer group, use the `no neighbor {ip-address | peer-group peer-group-name}` command.

To disable dmzlink-dw for the peer group, use the `no neighbor ip-address dmzlink-dw` 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.
- `dmzlink-bw` Enter the keyword `dmzlink-bw` to attach a link bandwidth to received routes.

**NOTE:** If `dmzlink-bw` is configured for a peer, in order for the BGP peer to advertise the prefixes with dmzlink-bw attached to it, you must reset the the peer or peer-group using the `clear ip bgp session` command.

Defaults

Not configured.

Command Modes

- **ROUTER BGP**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the dmzlink-bw parameter.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the S9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group’s configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- `neighbor advertisement-interval`
- `neighbor distribute-list`
- `neighbor route-map`
neighbor route-reflector-client

If a neighbor’s configuration is more specific than its peer group’s configuration, the neighbor may retain its configuration after it is added to the peer group. The neighbor’s configuration does not affect outgoing updates.

A peer group must exist (be enabled) before you add a peer to it. If the peer group is disabled (shutdown), the peers within that group are also disabled (shutdown).

In BGP, you cannot associate a peer to a peer-group without configuring the remote-as for Internal BGP (IBGP) or External BGP (EBGP).

This command automatically restarts the neighbor session for the configuration to take effect.

Related Commands

- `clear ip bgp` — reset BGP sessions.
- `neighbor peer-group (creating group)` — create a peer group.
- `show ip bgp peer-group` — view BGP peers.
- `show ip bgp neighbors` — view 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

**Command History**

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

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P6) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.
Usage Information
When you create a peer group, it is disabled (Shut mode).

Related Commands
• neighbor peer-group (assigning peers) — assign routers to a peer group.
• neighbor remote-as — assign a indirectly connected AS to a neighbor or peer group.
• neighbor shutdown — disable a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

Syntax
neighbor peer-group-name peer-group passive [limit sessions]

To delete a passive peer-group, use the no neighbor peer-group-name peer-group passive command.

Parameters
peer-group-name Enter a text string up to 16 characters long as the name of the peer group.

limit (Optional) Enter the keyword limit to constrain the numbers of sessions for this peer-group. The range is from 2 to 256. The default is 256.

Defaults
Not configured.

Command Modes
ROUTER BGP

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.8.0 Introduced the limit keyword on the S4810.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.
7.7.1.0 Introduced on the C-Series.

Usage Information
After you configure a peer group as passive, assign it a subnet using the neighbor soft-reconfiguration inbound command.

For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.

Related Commands
• neighbor soft-reconfiguration inbound — assign a subnet to a dynamically configured BGP neighbor.
neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

Syntax

neighbor {ip-address | peer-group-name} remote-as number

To delete a remote AS entry, use the no neighbor {ip-address | peer-group-name} remote-as number command.

Parameters

- **ip-address**: Enter the IP address of the neighbor to enter the remote AS in its routing table.
- **peer-group-name**: Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
- **number**: Enter a number of the AS. The range is from 0 to 65535 (2 byte) or from 1 to 4294967295 (4 byte).

Defaults

Not configured.

Command Modes

- ROUTER BGP

Command History

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

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series. Added 4-byte support.

Usage Information

To accept 4-byte formats before entering a 4 byte AS Number, configure your system. If the number parameter is the same as the AS number used in the router bgp command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (Shutdown).

This command automatically restarts the neighbor session for the configuration to take effect.

Related Commands

- **router bgp** — enter ROUTER BGP mode and configures routes in an AS.
- **bgp four-octet-as-support** — enable 4-byte support for the BGP process.
neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax

neighbor {ip-address | peer-group-name} remove-private-as

To return to the default, use the no neighbor {ip-address | peer-group-name} remove-private-as command.

Parameters

- ip-address
  Enter the IP address of the neighbor to remove the private AS numbers.
- peer-group-name
  Enter the name of the peer group to remove the private AS numbers.

Defaults

Disabled (that is, private AS number are not removed).

Command Modes

ROUTER BGP

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.
7.7.1.0 Introduced on the C-Series. Added 4-byte support.

Usage Information

Applies to EBGP neighbors only.

Configure your system to accept 4-byte formats before entering a 4 byte AS Number.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are from 64512 to 65535 (2 byte).
neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax

neighbor {ip-address | peer-group-name} route-map map-name {in | out}

To remove the route map, use the no neighbor {ip-address | peer-group-name} route-map map-name {in | out} command.

Parameters

- **ip-address**: Enter the IP address of the neighbor in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group.
- **map-name**: Enter the name of an established route map.

If the Route map is not configured, the default is deny (to drop all routes).

- **in**: Enter the keyword in to filter inbound routes.
- **out**: Enter the keyword out to filter outbound routes.

**NOTE**: This command sends routes to peers only if an outbound policy is configured and if there is a change in the existing outbound policy.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

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**

```plaintext
neighbor {ip-address | peer-group-name} route-reflector-client
```

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group.

**Defaults**

Not configured.

**Command Modes**

- `ROUTER BGP`

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not to be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster.
When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

This command automatically restarts the neighbor session for the configuration to take effect.

**Related Commands**
- `bgp client-to-client reflection` — enable route reflection between the route reflector and the clients.

**neighbor sender-side-loopdetect**

Enables sender-side loop detection for BGP.

**Syntax**
```
neighbor {ip-address | peer-group-name} sender-side-loopdetect
```

To disable sender-side loop detection, use the `no neighbor {ip-address | peer-group-name} sender-side-loopdetect` 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 enable or disable all routers with in the peer group. All routers in the peer group receive routes from a route reflector.

**Defaults**
Enabled.

**Command Modes**
ROUTER BGP

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
This command enables sender-side-loopdetect for a specified BGP neighbor. BGP does not advertise a route to a peer if the AS-Path of the route already contains the peer's AS.

**NOTE:** If you configure a neighbor to accept such routes using the `neighbor allowas-in` command, you must disable sender-side loop detection for that neighbor.
**neighbor send-community**

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

**Syntax**

neighbor {ip-address | peer-group-name} send-community [extended | standard]

To disable sending a COMMUNITY attribute, use the no neighbor {ip-address | peer-group-name} send-community command.

**Parameters**

- **ip-address**
  - Enter the IP address of the peer router in dotted decimal format.

- **peer-group-name**
  - Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

- **extended**
  - (OPTIONAL) Enter the keyword extended to send extended community attribute.

- **standard**
  - (OPTIONAL) Enter the keyword standard to send standard community attribute.

**Defaults**

Not configured and COMMUNITY attributes are not sent to neighbors.

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td><strong>Version 9.0.2.0</strong></td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To configure a COMMUNITY attribute, use the set community command in ROUTE-MAP mode.

In order that settings corresponding to the neighbor send-community command take effect, you must execute the clear ip bgp command immediately after you execute the neighbor send-community command.

If you do not set any of the optional parameters (standard or extended), then both standard as well as extended attributes are sent. If you set either the standard or extended parameter, only the attribute that is specified is sent.
neighbor shutdown

Disable a BGP neighbor or peer group.

Syntax

```
neighbor {ip-address | peer-group-name} shutdown

To enable a disabled neighbor or peer group, use the neighbor {ip-address | peer-group-name} no shutdown command.
```

Parameters

- `ip-address`: Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shut down, use the `show ip bgp summary` command to confirm its status.

Related Commands

- `show ip bgp summary` — display the current BGP configuration.
- `show ip bgp neighbors` — display the current BGP neighbors.
**neighbor soft-reconfiguration inbound**

Enable soft-reconfiguration for BGP.

**Syntax**

```plaintext
neighbor {ip-address | peer-group-name} soft-reconfiguration inbound
```

To disable, use the no neighbor {ip-address | peer-group-name} soft-reconfiguration inbound command.

**Parameters**

- `ip-address` Enter the IP address of the neighbor in dotted decimal format.
- `peer-group-name` Enter the name of the peer group to disable or enable all routers within the peer group.

**Defaults**

Disabled

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates the neighbor receives but does not reset the peer-session.

You cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.

⚠️ **CAUTION:** Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

🛠️ **NOTE:** This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

**Related Commands**

- `show ip bgp neighbors` — display routes received by a neighbor.
neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax

```
neighbor {ip-address | peer-group-name} timers keepalive holdtime
```

To return to the default values, use the no neighbor {ip-address | peer-group-name} timers command.

Parameters

- **ip-address**: Enter the IP address of the peer router in dotted decimal format.
- **peer-group-name**: Enter the name of the peer group to set the timers for all routers within the peer group.
- **keepalive**: Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is 60 seconds.
- **holdtime**: Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is 180 seconds.

Defaults

- keepalive = 60 seconds
- holdtime = 180 seconds

Command Modes

- ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

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
neighbo*r update-source

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax

```plaintext
neighbor {ip-address | peer-group-name} update-source interface
```

To use the closest interface, use the no neighbor {ip-address | peer-group-name} update-source interface command.

Parameters

- `ip-address`: Enter the IP address of the peer router in dotted decimal format.
- `peer-group-name`: Enter the name of the peer group to disable all routers within the peer group.
- `interface`: Enter the keyword `loopback` then a number of the Loopback interface. The range is from 0 to 16383.

Defaults

Not configured.

Command Modes

- ROUTER BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

Neighbors are sorted according to the source and destination ip addresses. If an update-source ip address exists, then the source ip address determines the order in which the neighbors are displayed.
neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax

neighbor {ip-address | peer-group-name} weight weight

To remove a weight value, use the no neighbor {ip-address | peer-group-name} weight command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Enter the IP address of the peer router in dotted decimal format.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Enter the name of the peer group to disable all routers within the peer group.</td>
</tr>
<tr>
<td>weight</td>
<td>Enter a number as the weight. The range is from 0 to 65535. The default is 0.</td>
</tr>
</tbody>
</table>

Defaults

0

Command Modes

ROUTER BGP

Command History

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

Version          Description          |
-----------------------------------------------|
9.8(1.0)          Introduced on the Z9100-ON. |
9.8(0.0P5)        Introduced on the S4048-ON. |
9.8(0.0P2)        Introduced on the S3048-ON. |
9.7(0.0)          Introduced on the S6000-ON. |
9.2(1.0)          Introduced on the Z9500. |
9.0.2.0           Introduced on the S6000. |
8.3.19.0          Introduced on the S4820T. |
8.3.11.1          Introduced on the Z9000. |
8.3.7.0           Introduced on the S4810. |
7.8.1.0           Introduced on the S-Series. |
7.7.1.0           Introduced on the C-Series. |

Usage Information

In the Dell Networking OS best path selection process, the path with the highest weight value is preferred.

NOTE: In the Dell Networking OS best-path selection process, the path with the highest weight value is preferred.

If you configure the set weight command in a route map applied to this neighbor, the weight set in that command overrides the weight set in the neighbor weight command.

Related Commands

- set weight — assign a weight to all paths meeting the route map criteria.
**network**

Specify the networks for the BGP process and enter them in the BGP routing table.

**Syntax**

```
network ip-address mask [route-map map-name]
```

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

**Parameters**

- **ip-address**
  
Enter an IP address in dotted decimal format of the network.

- **mask**
  
Enter the mask of the IP address in the slash prefix length format (for example, /24).

  The mask appears in command outputs in dotted decimal format (A.B.C.D).

- **route-map map-name**
  
  (OPTIONAL) Enter the keyword `route-map` then the name of an established route map.

  Only the following ROUTE-MAP mode commands are supported:
  - `match ip address`
  - `set community`
  - `set local-preference`
  - `set metric`
  - `set next-hop`
  - `set origin`
  - `set weight`

  If the route map is not configured, the default is `deny` (to drop all routes).

**Defaults**

Not configured.

**Command Modes**

- ROUTER BGP

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
Dell Networking OS software resolves the network address the network command configures with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes. As BGP does not query next-hop information corresponding to locally originated routes, a local route with an unreachable next-hop is chosen as the best route.

When a combination of locally originated and peer originated routes occurs, both these routes will exist in the RTM. However, only the best route is kept active in the RTM and the remaining route is rendered inactive.

It is possible to keep only one locally originated route in the BGP database. Network command has preference over the re-distributed routes. When the locally originated route is no longer present in the database the other route is automatically installed.

In BGP, the next-hop for the route is calculated from the information that is acquired through IGP or static routes.

Related Commands

- redistribute — redistribute 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

**Command History**

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

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
**permit bandwidth**

Enables you to specify link band width extended-community attribute as the matching criteria to permit incoming or outgoing traffic.

**Syntax**

```
permit bandwidth
```

To disable this setting, enter the `no permit bandwidth` command.

**Parameters**

- `bandwidth` Enter the keyword bandwidth to specify extended-community attribute as the matching criteria for permitting traffic. The range is from 0 to 102400.

**Defaults**

N/A

**Command Modes**

EXTENDED COMMUNITY LIST

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `deny bandwidth` – link band width extended-community attribute as the matching criteria to deny incoming or outgoing traffic.

**redistribute**

Redistribute routes into BGP.

**Syntax**

```
redistribute {connected | static} [route-map map-name]
```

To disable redistribution, use the `no redistribute {connected | static} command.

**Related Commands**

- `redistribute ospf` — Redistribute OSPF routes into BGP.
Parameters

connected Enter the keyword connected to redistribute routes from physically connected interfaces.

static Enter the keyword static to redistribute manually configured routes. These routes are treated as incomplete routes.

route-map map-name (OPTIONAL) Enter the keyword route-map then the name of an established route map.

Only the following ROUTE-MAP mode commands are supported:

- match ip address
- set community
- set local-preference
- set metric
- set next-hop
- set origin
- set weight

If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.3.1.0 Introduced the ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as internal.
7.8.1.0 Introduced on the S-Series.
7.7.1.0 Introduced on the C-Series.

Usage Information You can use the redistribute command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as MED.
If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.

As BGP does not query next-hop information corresponding to locally originated routes, a local route with an unreachable next-hop is chosen as the best route.

When a combination of locally originated and peer originated routes occurs, both these routes will exist in the RTM. However, only the best route is kept active in the RTM and the remaining route is rendered inactive.

It is possible to keep only one locally originated route in the BGP database. Network command has preference over the re-distributed routes. When the locally originated route is no longer present in the database the other route is automatically installed.

### Related Commands
- `neighbor default-originate` — inject 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**

- `process-id` Enter the number of the OSPF process. The range is from 1 to 65535.
- `match external {1 | 2}` (OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
- `match internal` (OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.
- `route-map map-name` (OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

**Defaults**

Not configured.

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100−ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048−ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048−ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000−ON.</td>
</tr>
</tbody>
</table>
router bgp

To configure and enable BGP, enter ROUTER BGP mode.

Syntax:
```
router bgp as-number
```

Parameters:

- `as-number`:
  
  Enter the AS number. The range is from 1 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults:

- Not enabled.

Command Modes:

- CONFIGURATION

Command History:

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

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.3.1.0 | Introduced on the S4820T.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.

Usage Information:

You can use the redistribute command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and apply outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as MED.

When you enter the redistribute isis process-id command without any other parameters, Dell Networking OS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. RFC does not support this feature.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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
```

BGP does not allow 23456 (AS-TRANS) as a configured AS number.

**Example**

```
Dell(conf)# router bgp 3
Dell(conf-router_bgp)#
```

### set extcommunity bandwidth

Enables you to set extended community bandwidth.

**Syntax**

```
set extcommunity bandwidth
```

To disable extended community bandwidth, enter the `no set extcommunity bandwidth` command.

**Parameters**

- `bandwidth`
  - Enter the keyword `bandwidth` to enable extended community bandwidth. The range is from 0 to 102400.

**Defaults**

N/A

**Command Modes**

ROUTER MAP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

A new policy command is introduced in order to attach the Link Bandwidth extended community only to the prefixes that are received from a neighbor that satisfy the desired conditions. This command is relevant for both inbound as well as outbound policy handling (for received prefixes). Also, there is no change to the set of supported conditions or filters.

During configuration, the bandwidth is specified in Mbps, not in bytes/second. While creating the actual LB extended community, the system will attach the AS number and encode the bandwidth in floating point format.
show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

Syntax

```
show capture bgp-pdu neighbor ipv4-address
```

Parameters

- **ipv4-address**: Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

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 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

[...]

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
```
**show config**

View the current ROUTER BGP configuration.

**Syntax**

```
show config
```

**Command Modes**

ROUTER BGP

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf-router_bgp)# show config
!
router bgp 100
 network 1.1.11.1/32
 network 1.1.12.1/32
 network 1.1.13.1/32
 neighbor 10.1.1.2 remote-as 200
 neighbor 10.1.1.2 no shutdown
Dell(conf-router_bgp)#
```

**show ip bgp**

View the current BGP IPv4 routing table for the system.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 unicast] [network [network-mask] [longer-prefixes]]
```
Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view ipv4-unicast route information corresponding to that VRF.
- **ipv4 unicast** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
- **network** (OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
- **network-mask** (OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
- **longer-prefixes** (OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

Command Modes

- **EXEC**
- **EXEC Privilege**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the ADDPATH parameters.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

In BGP, this command displays the exact reason why the route is discarded.

The following describes the `show ip bgp` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
</tbody>
</table>
### Field Description

- **Weight**
  Displays the route’s weight.

- **Path**
  Lists all the ASs the route passed through to reach the destination network.

The `show ip bgp` command displays the dmzlink-dw details only if dmzlink-bw is enabled using the `bgp dmzlink-dw` command.

#### Example

```plaintext
Dell# show ip bgp
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 55.0.0.0/24</td>
<td>172.16.0.2</td>
<td></td>
<td>0</td>
<td>200</td>
<td>i</td>
</tr>
<tr>
<td>*&gt; 66.0.0.0/24</td>
<td>172.16.0.2</td>
<td></td>
<td>0</td>
<td>200</td>
<td>i</td>
</tr>
</tbody>
</table>
```

All the show and debugs commands display the link band width extended-community prefixed with DMZ-Link-bw along with other extended communities.

```plaintext
Dell# show ip bgp 3.3.3.0/24
BGP routing table entry for 3.3.3.0/24
Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from : 1.1.1.2 (3.3.3.1) Best
AS PATH :
Next-Hop : 1.1.1.2, Cost : 0
Origin IGP, Metric 0, LocalPref 100, Weight 0, internal
Extended Communities :
DMZ-Link Bw: 2000 kbytes*
```

#### Related Commands

- `show ip bgp community` — view the BGP communities.
- `neighbor maximum-prefix` — control the number of network prefixes received.

---

### show ip bgp cluster-list

View BGP neighbors in a specific cluster.

#### Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] cluster-list [cluster-id]
```

#### Parameters

- **vrf vrf-name**
  (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view cluster information of BGP neighbors corresponding to that VRF.

- **ipv4 multicast**
  (OPTIONAL) Enter the keywords `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.

- **ipv4 unicast**
  (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 unicast  (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to view information related to only to the ipv6 unicast routes.

cluster-id  (OPTIONAL) Enter the cluster id in dotted decimal format. The range is 1 — 4294967295.

Command Modes
- EXEC
- EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the ipv4 multicast and ipv6 unicast parameters.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The following describes the show ip bgp cluster-list command shown in the following example.

Field                  Description
Network                Displays the destination network prefix of each BGP route.
Next Hop               Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric                 Displays the BGP route's metric, if assigned.
LocPrf                 Displays the BGP LOCAL_PREF attribute for the route.
Weight                 Displays the route's weight.
Path                   Lists all the ASs the route passed through to reach the destination network.

Example

Dell# show ip bgp cluster-list
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.6
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*I 55.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0 400 500 600 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*I 66.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0 500 i</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*I 77.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0 i</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Border Gateway Protocol
Dell# show ip bgp cluster-list 4.4.4.4
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.6
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;I 55.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0</td>
<td>400</td>
<td>500</td>
</tr>
<tr>
<td>*&gt;I 66.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0</td>
<td>500</td>
<td>i</td>
</tr>
<tr>
<td>*&gt;I 77.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>0</td>
<td>i</td>
<td></td>
</tr>
</tbody>
</table>

Dell#

**show ip bgp community**

View information on all routes with Community attributes or view specific BGP community groups.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
community [community-number] [local-as] [no-export] [no-advertise]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view information either on all routes with community attributes or specific BGP community routes corresponding to that VRF.
- `ipv4 unicast` (OPTIONAL) Enter the keywords `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
- `ipv4 multicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
- `ipv6 unicast` (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
- `community-number` Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
  
  You can specify up to eight community numbers to view information on those community groups.
- `local-AS` Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED.
  
  All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
- `no-advertise` Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE.
  
  All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
- `no-export` Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT.
All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the ipv4 multicast and ipv6 unicast parameters.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip bgp community?
local-AS     Do not export outside local AS (well-known community)
no-advertise Do not advertise to any peer (well-known community)
no-export    Do not export to next AS (well-known community)
a:nn         Community number in as:nn format
| Pipe through a command
```
show ip bgp community

Dell# show ip bgp community
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 55.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>200</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>* 66.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>200</td>
<td></td>
<td>i</td>
</tr>
</tbody>
</table>

Dell# show ip bgp community no-advertise
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 66.0.0.0/24</td>
<td>172.16.0.2</td>
<td>0</td>
<td>200</td>
<td></td>
<td>i</td>
</tr>
</tbody>
</table>

Dell#

**show ip bgp community-list**

View routes that a specific community list affects.

**Syntax**

```
show ip bgp [vrf vrf-name] {ipv4 {unicast | multicast} | ipv6 unicast} community-list community-list-name [exact-match]
```

**Parameters**

- **vrf vrf-name** *(OPTIONAL)* Enter the keywords vrf and then the name of the VRF to view routes affected by a specific community list corresponding to that VRF.
- **ipv4 unicast** *(OPTIONAL)* Enter the keywords ipv4 unicast to view information only related to ipv4 unicast routes.
- **ipv4 multicast** *(OPTIONAL)* Enter the keyword ipv4 followed by the keyword multicast to view information related only to ipv4 multicast routes.
- **ipv6 unicast** *(OPTIONAL)* Enter the keyword ipv6 followed by the keyword unicast to view information related only to ipv6 unicast routes.
- **community-list-name** Enter the name of a configured IP community list (maximum 140 characters).
- **exact-match** Enter the keyword for an exact match of the communities.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
**Usage Information**

The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community-list pass` command shown in the following example.

**Field** | **Description**
---|---
**Network** | Displays the destination network prefix of each BGP route.
**Next Hop** | Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
**Metric** | Displays the BGP route's metric, if assigned.
**LocPrf** | Displays the BGP LOCAL_PREF attribute for the route.
**Weight** | Displays the route's weight.
**Path** | Lists all the ASs the route passed through to reach the destination network.

**Example**

```
Dell(conf)# ip community-list cl1
Dell(config-community-list)# permit 1000:1
Dell(config-community-list)# end

Dell# show ip bgp community-list cl1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                                 0 200 i

Dell# show ip bgp 55.0.0.0/24
BGP routing table entry for 55.0.0.0/24
Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer

Received from : 172.16.0.2 (172.16.0.2)  Best
   AS_PATH : 200
   Next-Hop  : 172.16.0.2, Cost : 0
   Origin IGP, Metric  4294967295 (Default), LocalPref  100, Weight  0, external

Communities :
   200:1        1000:1       3000:1
Dell#
```
**show ip bgp dampened-paths**

View BGP routes that are dampened (non-active).

**Syntax**
```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] dampened-paths
```

**Parameters**
- **vrf vrf-name**  (OPTIONAL) Enter the keywords vrf and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
- **ipv4 multicast**  (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to view information related only to ipv4 multicast routes.
- **ipv4 unicast**  (OPTIONAL) Enter the keywords ipv4 followed by the keyword unicast to view information related only to ipv4 unicast routes.
- **ipv6 unicast**  (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to view information related only to ipv6 unicast routes.

**Command Modes**
- EXEC
- EXEC Privilege

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

**Version**
- 9.8(1.0) Introduced on the Z9100-ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Added the ipv4 multicast and ipv6 unicast parameters.
- 9.4(0.0) Added support for VRF.
- 9.2(1.0) Introduced on the Z9500.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.11.1 Introduced on the Z9000.
- 8.3.7.0 Introduced on the S4810.
- 7.8.1.0 Introduced on the S-Series.
- 7.7.1.0 Introduced on the C-Series.

**Usage Information**
To determine a BGP session flap, both a route-down event and a subsequent route-up event corresponding to a single route are considered. As a result, a flap event is penalized only one time during the route-down event. The subsequent route-up event corresponding to the same route is not considered as a flap and is not penalized.
The history paths that the `show ip bgp` command displays contain only the prefix and the next-hop information. The next-hop information shows the IP address of the neighbor. It does not show the actual next-hop details.

The following describes the `show ip bgp damp` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the dampened route.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hour:minutes:seconds until the dampened route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the dampened route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip bgp dampened-paths
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
          n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            From            Reuse     Path
d   55.0.0.0/24      172.16.0.2             00:36:23      200
```

**show ip bgp detail**

Display BGP internal information for the IPv4 Unicast address family.

**Syntax**

```
show ip bgp [ipv4 unicast] detail
```

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.
7.5.1.0 | Introduced.

Example

Dell# show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdFics 74857 :
NhLocAs 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfDid 0 : NdMedMissVal -1 :
NdIgrnIId 0 : NdRRC2C 1 : NdListId 33686273 : NdPsTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRC2Cp 0x41a190a8
NdPfxPA 0 : NdLocCmpP 0x41a6f000 : NdTmpPAP 0x41a6f000 : NdTmpA2PAP 0x41a6f000 :
NdTempComdp 0x41a25b80
NdTmRpCRCp 0x41a4b000 : NdTmpOptP 0x41a4b000 : NdTmpNhP 0x41a4b000 : NdOrigAPF 0
NdOrigNHp 0 : NdModPathP 0x419efcc0 : NdModAspAP 0x41a4c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNhP : NdModNhP : NdComSortBufP 0x41a19010 : NdComSortHdp
0x41a190d4 : NdPdpAPFmk 0 : APFstset 0x41a1a298 : NhospDfrdHdp 0x41a1a3e0:
NumNhDfrd 0 : CfgHdrAPFmk 1
APCHwNetTmrP 0x41a1e75c : AFRttDamp 0 : AlwysCmpMed 0 : LocrRld 10 : LocrRem 10 :
softReconfig 0x41a1a38c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a1d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fails 0 : ConnExps 0 : KeepExps 0 : SoftRst 0 : RxOpens 0 :
RxKeeps 0 : RxUpdgs 0 : RxRtifs 0 : TxUpdgs 0 : TxRtifs 0
BadEvts 0 : SynFails 0 : RxRttCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxRttCodeP 0x41a1b734 : TxHdrCodeP 0x41a1b750 : TxOptPap 0:
0x41a1b760
TxUpdOptP 0x41a1b780 : TrEvts 0 : LocPref 100 : tmpPathP 0x41a1b78 : LogNbrChgs 1
RecursiveNh 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 : AgrpVallmrp 0
0x41a1e7024
UpdNetTmrP 0x41a1e7094 : PeerChgRmTmrP 0 : CleanRibTmrP 0x41a1e7094
PeerUpdTmrP 0x41a1e70c3 : DfrdNhTmrP 0x41a1e7174 : DfrdRtscelTmrP 0x41a1e73c :
FastExtFallover 1 : FastIntFallover 0 : EnforceLstAS 1
PeerIdBitsP 0x419e7120 : softOutSz 16 : RibUpdCtxtCBP 0
UpdPeerCtxtCBP 0 : UpdPeerCtxtAPF 0 : TcpcpCtxtCB 0 : RedistBlk 1
NextCBpurg 110111536 : NumPeerToPurge 0 : PeerRtscelTmrP 0 : NonDet 0 : DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdRtmestmp 0 : SmpTrps 0 : IgrrBestPthASp 0
RstOn 1 : RstMod 1 : RstRole 2 : APFals 7 : RstInt 120 : MaxxorExtInt 361
FixedPrcart 1 : VarPrcart 1
Packet Capture max allowed length 40960000 : current length 0
Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AfIndex 0
NhspDpiflag 0x41a190b0 : AFRttP 0x41a190d200 : NdRtMMkp 0x41a19d28 : NdRtMafTb1Ver 0 :
NdRbCtxtAddr 1101110688
NdRbCtxtAddrLen 255 : NdAfPfx 0 : NdAfNrr 0 : NdAfNrrLen 0 : NdAfNrrPTr 0
NdAfNHn 0 : NdAfNHn : NdAfNhRedRttP 0x41a1d400 : NdNhCtxtAdd 1101110688
NdRedCtxtAddLen 255 : NdAfRedMkP 0x41a19e88 : AFAggCtxtP 0x41a0d600 : AFAggCtxtAddr
110111028 : AFAggCtxtAddLen 255
AfNumAggrFpx 0 : AfNumAggrAsS 0 : AfNumSupmap 0 : AfNumAggrValidPfx 0 :
AfNumPathBmp 0x41a1d700
MpathCtxtAddr 1101111140 : MpathCtxtAddrlen 255 : AfEorSet 0x41a19f98 : NumDfrdFpx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 110112312 : AfIntDist 200 : AfLocDist 200
AfNumRtr 0 : AFR 0 : AFR 0 : AFRTt 0x41a1d300 : AFRtCtxtAddr 110112392 :
AFLerCtxtAddrlen 255
AFLerCtxtAddr 110112443 : AFLerCtxtAddrlen 255 : AFLerBkDrRttP 0x41a1d500 :
AFLerBkDrCtxtAddr 0 : AFDmpHlife 0
AFDmpRvse 0 : AFDmpSupp 0 : AFDmpMaxHld 0 : AFDmpCeiling 0 : AFDmpMapP
Dell#
**show ip bgp extcommunity-list**

View information on all routes with Extended Community attributes.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
extcommunity-list [list name]
```

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keywords vrf and then the name of the VRF to view information on all routes with extended community attributes corresponding to that VRF.
- **ipv4 multicast** (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to view information related only to ipv4 multicast routes.
- **ipv4 unicast** (OPTIONAL) Enter the keywords ipv4 unicast to view information only related to ipv4 unicast routes.
- **ipv6 unicast** (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to view information related only to ipv6 unicast routes.
- **list name** Enter the extended community list name you wish to view. The range is 140 characters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the ipv4 multicast and ipv6 unicast parameters.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.
The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

**Example**

```
Dell# show run extcommunity-list
!
ip extcommunity-list ecl1
  permit rt 100:4
  permit soo 40:4
Dell# show ip bgp extcommunity-list ecl1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network             Next Hop            Metric     LocPrf Weight Path
*>   55.0.0.0/24        172.16.0.2                                 0 200 i
*>   77.0.0.0/24        172.16.0.2                                 0 200 i
Dell# show ip bgp extcommunity-list ec
% Error: Extended community list does not exist.
Dell#
```

**show ip bgp filter-list**

View the routes that match the filter lists.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] filter-list as-path-name
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view route information that matches the filter lists corresponding to that VRF.
- `ipv4 multicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
- `ipv4 unicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
- `ipv6 unicast` (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
- `as-path-name` Enter an AS-PATH access list name. The range is 140 characters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
### Version Description

9.7(0.0)  
Added the ipv4 multicast and ipv6 unicast parameters.

9.4.(0.0)  
Added support for VRF.

9.2(1.0)  
Introduced on the Z9500.

9.0.2.0  
Introduced on the S6000.

8.3.19.0  
Introduced on the S4820T.

8.3.11.1  
Introduced on the Z9000.

8.3.7.0  
Introduced on the S4810.

7.8.1.0  
Introduced on the S-Series.

7.7.1.0  
Introduced on the C-Series.

### Usage Information

The following describes the `show ip bgp filter-list hello` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path source codes</td>
<td>Lists the path sources shown to the right of the last AS number in the Path column:</td>
</tr>
<tr>
<td></td>
<td>• i = internal route entry</td>
</tr>
<tr>
<td></td>
<td>• a = aggregate route entry</td>
</tr>
<tr>
<td></td>
<td>• c = external confederation route entry</td>
</tr>
<tr>
<td></td>
<td>• n = network route entry</td>
</tr>
<tr>
<td></td>
<td>• r = redistributed route entry</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>Displays the BGP route's metric, if assigned.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>Displays the route's weight.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show run as-path al
!
ip as-path access-list al
    permit 500
Dell# show ip bgp filter-list a1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
            n - network, D - denied, S - stale
Origin codes: I - IGP, e - EGP, ? - incomplete

               Network       Next Hop        Metric     LocPrf Weight Path
*:55.0.0.0/24   172.16.0.2       0 200 400 500 600 i
*:66.0.0.0/24   172.16.0.2       0 200 500 i
Dell#
```
**show ip bgp flap-statistics**

View flap statistics on BGP routes.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] flap-statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-expression]
```

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view flap statistics on BGP routes corresponding to that VRF.
- **ipv4 multicast** (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
- **ipv4 unicast** (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
- **ipv6 unicast** (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
- **ip-address** (OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
- **mask** (OPTIONAL) Enter the network mask (in slash prefix `/x` format) of the BGP network address.
- **filter-list as-path-name** (OPTIONAL) Enter the keyword `filter-list` then the name of a configured AS-PATH ACL. The range is 140 characters.
- **regexp regular-expression** Enter a regular expression then use one or a combination of the following characters to match. The range is 256 characters.
  - . = (period) any single character (including a white space).
  - * = (asterisk) the sequences in a pattern (zero or more sequences).
  - + = (plus) the sequences in a pattern (one or more sequences).
  - ? = (question mark) sequences in a pattern (either zero or one sequences).

- **NOTE:** Enter an escape sequence (CTRL+v) prior to entering the regular expression.
  - [ ] = (brackets) a range of single-character patterns.
  - ( ) = (parenthesis) groups a series of pattern elements to a single element.
  - { } = (braces) minimum and the maximum match count.
  - ^ = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

**Command Modes**
- EXEC
- EXEC Privilege
show ip bgp inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax

show ip bgp [vrf vrf-name] [ipv4 unicast] inconsistent-as
Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view routes corresponding to the VRF that contain inconsistent originating AS numbers.
- **ipv4 unicast** (OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the `show ip bgp inconsistent-as` command shown in the following example.

**Field**  
**Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP route's metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route's weight.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

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
* 3.0.0.0/8  63.114.8.34  0 18508 209 7018 80 i
* 3.0.0.0/8  63.114.8.60  0 18508 209 7018 80 i
*> 3.0.0.0/8  63.114.8.33  0 18508 701 80 i
```

Border Gateway Protocol | 413
show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.

Syntax

show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] neighbors [ip-address [advertised-routes | dampened-routes | detail | flap-statistics | routes | [received-routes [network [network-mask]]] | [denied-routes [network [network-mask]]]]

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf and then the name of the VRF to view information exchanged by BGP neighbors corresponding to that VRF.

NOTE: You can use this attribute to view information exchanged by BGP neighbors that correspond to either a default or a non-default VRF.

ipv4 multicast  (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to view information related only to ipv4 multicast routes.

ipv4 unicast  (OPTIONAL) Enter the keyword ipv4 followed by the keyword unicast to view information related only to ipv4 unicast routes.

ipv6 unicast  (OPTIONAL) Enter the keyword ipv6 followed by the keyword unicast to view information related only to ipv6 unicast routes.
ip-address  (OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.

advertised-routes  (OPTIONAL) Enter the keywords advertised-routes to view only the routes the neighbor sent.

dampened-routes  (OPTIONAL) Enter the keywords dampened-routes to view information on dampened routes from the BGP neighbor.

detail  (OPTIONAL) Enter the keyword detail to view neighbor-specific internal information for the IPv4 Unicast address family.

flap-statistics  (OPTIONAL) Enter the keywords flap-statistics to view flap statistics on the neighbor’s routes.

routes  (OPTIONAL) Enter the keyword routes to view only the neighbor’s feasible routes.

received-routes  [network [network-mask]]  (OPTIONAL) Enter the keywords received-routes then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors.

   NOTE: Configure the neighbor soft-reconfiguration inbound command prior to viewing all the information received from the neighbors.

denied-routes  [network [network-mask]]  (OPTIONAL) Enter the keywords denied-routes then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

Version  Description

9.8(1.0)   Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)   Added the ipv4 multicast and ipv6 unicast parameters.
9.0.2.0     Introduced on the S6000.
8.3.19.0    Introduced on the S4820T.
8.3.11.1    Introduced on the Z9000.
8.3.8.0     Added the add-path option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0     Introduced on the S4810.
7.8.1.0     Introduced on the S-Series.
7.7.1.0     Introduced on the C-Series.
7.5.1.0     Added the detail option. Output now displays the default MED value.
7.2.1.0     Added the received and denied route options.
6.3.10      The output is changed to display the total number of advertised prefixes.
After a peer reset, the contents of the notification log messages is displayed in hex values for debugging.

The neighbor information that this command displays does not include counts corresponding to ignored prefixes and updates. However, the martian case is an exception where neighbor information corresponding to ignored updates is displayed.

BGP shows the exact information that is exchanged between the BGP peers. It also indicates whether or not this information is received by the BGP peer.

The following describes the `show ip bgp neighbors` command shown in the following examples.

<table>
<thead>
<tr>
<th>The Lines Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>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.</td>
</tr>
<tr>
<td>BGP version</td>
<td>Displays the BGP version (always version 4) and the remote router ID.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Displays the neighbor’s BGP state and the amount of time in hours:minutes:seconds it has been in that state.</td>
</tr>
<tr>
<td>Last read</td>
<td>This line displays the following information:</td>
</tr>
<tr>
<td></td>
<td>• last read is the time (hours:minutes:seconds) the router read a message from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• hold time is the number of seconds configured between messages from its neighbor</td>
</tr>
<tr>
<td></td>
<td>• keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.</td>
</tr>
<tr>
<td>Received messages</td>
<td>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.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>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.</td>
</tr>
<tr>
<td>Received updates</td>
<td>This line displays the number of BGP updates received and sent.</td>
</tr>
<tr>
<td>Soft reconfiguration</td>
<td>This line indicates that soft reconfiguration inbound is configured.</td>
</tr>
<tr>
<td>Minimum time</td>
<td>Displays the minimum time, in seconds, between advertisements.</td>
</tr>
<tr>
<td>(list of inbound and outbound policies)</td>
<td>Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.</td>
</tr>
<tr>
<td>For address family</td>
<td>Displays the IPv4 Unicast as the address family.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays which version of the primary BGP routing table the router and the neighbor are using.</td>
</tr>
<tr>
<td>accepted prefixes</td>
<td>Displays the number of network prefixes the router accepts and the amount of memory used to process those prefixes.</td>
</tr>
<tr>
<td>Prefix advertised</td>
<td>Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.</td>
</tr>
<tr>
<td>Last reset</td>
<td>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.</td>
</tr>
</tbody>
</table>
The Lines
Beginning with:

Local host: Displays the peering address of the local router and the TCP port number.
Foreign host: Displays the peering address of the neighbor and the TCP port number.

Example

Dell# show ip bgp neighbors 172.16.0.2
BGP neighbor is 172.16.0.2, remote AS 200, external link
  Member of peer-group port0 for session parameters
  BGP remote router ID 172.16.0.2
  BGP state ESTABLISHED, in this state for 00:13:55
  Last read 00:00:03, Last write 00:00:55
  Hold time is 180, keepalive interval is 60 seconds
  Received 50 messages, 0 in queue
    1 opens, 0 notifications, 34 updates
    15 keepalives, 0 route refresh requests
  Sent 18 messages, 0 in queue
    1 opens, 0 notifications, 0 updates
    16 keepalives, 0 route refresh requests
  Route refresh request: received 0, sent messages 1
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds
  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)

  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ADD_PATH(69)
    CISCO_ROUTE_REFRESH(128)

For address family: IPv4 Unicast
  BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
  InQ : Added 0, Replaced 0, Withdrawn 0
  OutQ : Added 0, Withdrawn 0
  Allow local AS number 0 times in AS-PATH attribute
  Prefixes accepted 2, withdrawn 15 by peer, martian prefixes ignored 0
  Prefixes advertised 0, denied 0, withdrawn 0 from peer

  Connections established 1; dropped 0
  Last reset never
  Local host: 172.16.0.1, Local port: 58145
  Foreign host: 172.16.0.2, Foreign port: 179

Dell#

Related Commands

- show ip bgp — view the current BGP routing table.
**show ip bgp next-hop**

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

**Syntax**

```
show ip bgp [vrf vrf-name] next-hop
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show ip bgp next-hop` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-hop</td>
<td>Displays the next-hop IP address.</td>
</tr>
<tr>
<td>Via</td>
<td>Displays the IP address and interface used to reach the next hop.</td>
</tr>
<tr>
<td>RefCount</td>
<td>Displays the number of BGP routes using this next hop.</td>
</tr>
<tr>
<td>Cost</td>
<td>Displays the cost associated with using this next hop.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Displays the number of times the next hop has flapped.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip bgp next-hop
             Next-hop    Resolved
         172.16.0.2       YES
Dell#
```
show ip bgp paths

View all the BGP path attributes in the BGP database.

Syntax

show ip bgp [vrf vrf-name] paths [regexp regular-expression]

Parameters

vrf vrf-name

(OPTIONAL) Enter the keyword vrf to view all path attributes in the BGP database corresponding to that VRF.

NOTE: Description
You can use this attribute to view information on all path attributes in the BGP database that correspond to either a default or a non-default VRF.

regexp regular-expression

Enter a regular expression then use one or a combination of the following characters to match:

- . = (period) any single character (including a white space).
- * = (asterisk) the sequences in a pattern (zero or more sequences).
- + = (plus) the sequences in a pattern (one or more sequences).
- ? = (question mark) sequences in a pattern (either zero or one sequences).

NOTE: Enter an escape sequence (CTRL+v) prior to entering the regular expression.

- [ ] = (brackets) a range of single-character patterns.
- ( ) = (parenthesis) groups a series of pattern elements to a single element.
- { } = (braces) minimum and the maximum match count.
- ^ = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- $ = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduces on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduces on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduces on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduces on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF for the S4810, S4820T, and S6000.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduces on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduces on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduces on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduces on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduces on the S4810.</td>
</tr>
</tbody>
</table>
### Usage Information

The following describes the `show ip bgp path` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of BGP path attributes.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using this path attribute.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the MED attribute for this path attribute.</td>
</tr>
<tr>
<td>Path</td>
<td>Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces () are AS_SET information.</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show ip bgp paths ?
community               Display community information
extcommunity            Display extended community information
regexp                  Display path information based on a regular expression
|                       Pipe through a command

Dell# show ip bgp paths
Total 2 Paths
Refcount Metric Path
 1       0           200 i
 1       0           200 i
Dell#
```

### show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

#### Syntax

```
show ip bgp [vrf vrf-name] paths community
```

#### Command Modes

- EXEC
- EXEC Privilege

#### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp paths community` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these communities.</td>
</tr>
<tr>
<td>Community</td>
<td>Displays the community attributes in this BGP path.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show ip bgp paths community
Total 2 communities
Refcount Community
1 NO-ADVERTISE
1 200:1 1000:1 3000:1
Dell#
```

`show ip bgp peer-group`

Allows you to view information on the BGP peers in a peer group.

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] peer-group [peer-group-name [detail | summary]]
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` to view information on BGP peers in a peer group corresponding to that VRF.
  
  **NOTE:** You can use this attribute to view information on BGP peers in a peer group that correspond to either a default or a non-default VRF.

- `ipv4 multicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.

- `ipv4 unicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.

- `ipv6 unicast` (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.

- `peer-group-name` (OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail  (OPTIONAL) Enter the keyword detail to view detailed status information of the peers in that peer group.

summary  (OPTIONAL) Enter the keyword summary to view status information of the peers in that peer group. The output is the same as that found in the show ip bgp summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Added the add-path option to the S4810. Output on the S4810 shows the ADDPATH parameters.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show ip bgp peer-group command shown in the following example.

**Line beginning with:**

- **Peer-group**
  - Displays the peer group’s name.
- **Administratively shut**
  - Displays the peer group’s status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
- **BGP version**
  - Displays the BGP version supported.
- **Minimum time**
  - Displays the time interval between BGP advertisements.
- **For address family**
  - Displays IPv4 Unicast as the address family.
- **BGP neighbor**
  - Displays the name of the BGP neighbor.
- **Number of peers**
  - Displays the number of peers currently configured for this peer group.
- **Peer-group members:**
  - Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

**Example**

Dell# show ip bgp peer-group
Peer-group port0, remote AS 200
BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is port0, peer-group external
Update packing has 4_OCTET_AS support enabled

Number of peers in this group 1
Maximum limit on the accepted connections 256

Peer-group members (* - outbound optimized):
172.16.0.2
Dell#

Related Commands
- neighbor peer-group (assigning peers) — assign a peer to a peer-group.
- neighbor peer-group (creating group) — create a peer group.

show ip bgp regexp

Display the subset of the BGP routing tables matching the regular expressions specified.

Syntax
show ip bgp [vrf vrf-name] regexp regular-expression [character]

Parameters
- vrf vrf-name
  Enter the keyword vrf and then the name of the VRF to view the subset of BGP routing tables that match the regular expression specified on that VRF.

  NOTE: You can use this attribute to view the subset of BGP routing tables that match the regular expression that is specified on either a default or a non-default VRF.

- regular-expression
  Enter a regular expression then use one or a combination of the following characters to match:
  - . = (period) any single character (including a white space).
  - * = (asterisk) the sequences in a pattern (zero or more sequences).
  - + = (plus) the sequences in a pattern (one or more sequences).
  - ? = (question mark) sequences in a pattern (either zero or one sequences).

  NOTE: Enter an escape sequence (CTRL+v) prior to entering the ? regular expression.
  - [ ] = (brackets) a range of single-character patterns.
  - ( ) = (parenthesis) groups a series of pattern elements to a single element.
  - { } = (braces) minimum and the maximum match count.
  - ^ = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
  - $ = (dollar sign) the end of the output string.

Command Modes
- EXEC
- EXEC Privilege

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

The following describes the `show ip bgp regexp` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the destination network prefix of each BGP route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>Displays the BGP router’s metric, if assigned.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Displays the BGP LOCAL_PREF attribute for the route.</td>
</tr>
<tr>
<td>Weight</td>
<td>Displays the route’s weight.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the AS paths the route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip bgp regexp ^200
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, b - denied, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network             Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                                 0 200 i
*>  66.0.0.0/24        172.16.0.2                                 0 200 i
```

Dell#

**show ip bgp summary**

Allows you to view the status of all BGP connections.

**Syntax**

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] summary
```
Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view the status of all BGP connections corresponding to that VRF.
- **ipv4 multicast** (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
- **ipv4 unicast** (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
- **ipv6 unicast** (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

In BGP, route attributes are maintained at different locations. When attributes that correspond to multiple routes change, then attribute counts that the `show ip bgp summary` command displays are calculated as summations of attributes corresponding to all the associated routes. For example, if `cluster:id` is an attribute associated with thousand routes that contain exactly the same set of attributes, then the `cluster:id` count is 1. If these thousand routes are set with different attribute values with the same `cluster:id`, then the `cluster:id` count is 1000, since the same value is stored for thousand different attribute records.

The attribute next-hop is a part of the BGP attribute data structure.

If two peers send the same route that contains similar path attributes, then two entries are maintained in the back-end, as both these entries have different next-hops. If this same route is sent to a different peer, an entry for each peer is created, as the next-hop is different. As a result, the BGP attributes count in the summary output will differ accordingly.

The following describes the `show ip bgp summary` command shown in the following example.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP router identifier</td>
<td>Displays the local router ID and the AS number.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Displays the BGP table version and the main routing table version.</td>
</tr>
<tr>
<td>network entries</td>
<td>Displays the number of network entries, route paths, and the amount of memory used to process those entries.</td>
</tr>
<tr>
<td>paths</td>
<td>Displays the number of paths and the amount of memory used.</td>
</tr>
<tr>
<td>denied paths</td>
<td>Displays the number of denied paths and the amount of memory used.</td>
</tr>
<tr>
<td>BGP path attribute entries</td>
<td>Displays the number of BGP path attributes and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP AS-PATH entries</td>
<td>Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.</td>
</tr>
<tr>
<td>BGP community entries</td>
<td>Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp community command provides more details on the COMMUNITY attributes.</td>
</tr>
<tr>
<td>Dampening enabled</td>
<td>Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the BGP neighbor address.</td>
</tr>
<tr>
<td>AS</td>
<td>Displays the AS number of the neighbor.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>Displays the number of BGP messages that neighbor received.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>Displays the number of BGP messages that neighbor sent.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Displays the version of the BGP table that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Displays the number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>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.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.</td>
</tr>
<tr>
<td>Time</td>
<td>Display Example</td>
</tr>
<tr>
<td>Established</td>
<td>00:12:23 (hours:minutes:seconds)</td>
</tr>
<tr>
<td></td>
<td>1d21h (Days:Hours)</td>
</tr>
<tr>
<td></td>
<td>11w2d (Weeks:Days)</td>
</tr>
<tr>
<td>State/Pfxrd</td>
<td>If the neighbor is in Established stage, the number of network prefixes received.</td>
</tr>
<tr>
<td></td>
<td>If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Field | Description
-- | --
If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

Dell\# show ip bgp summary
BGP router identifier 192.168.11.5, local AS number 100
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
2 network entrie(s) using 152 bytes of memory
2 paths using 208 bytes of memory
BGP-RIB over all using 210 bytes of memory
2 BGP path attribute entrie(s) using 144 bytes of memory
1 BGP AS-PATH entrie(s) using 10 bytes of memory
2 neighbor(s) using 16384 bytes of memory

Neighbor | AS | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down | State/Pfx
--------- | -- | ------ | ------ | ------ | --- | --- | ------- | -------
172.16.0.2 | 200 | 10 | 8 | 0 | 0 | 0 | 00:05:34 | 2
192.168.10.2 | 100 | 0 | 22 | 0 | 0 | 0 | 00:00:00 (shut)

Dell#

show running-config bgp

To display the current BGP configuration, use this feature.

Syntax

show running-config bgp

Defaults

none

Command Modes

EXEC Privilege

Command History

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

Version | Description
--------- | --------
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.7.1.0 | Introduced on the C-Series.
7.6.1.0 | Introduced on the E-Series.

Example

Dell# show running-config bgp

! router bgp 100
   network 1.1.11.1/32
   network 1.1.12.1/32
   network 1.1.13.1/32
   neighbor 10.1.1.1.2 remote-as 200
   neighbor 10.1.1.2 no shutdown

Dell#
**timers bgp**

Adjust the BGP Keep Alive and Hold Time timers.

**Syntax**

```
timers bgp keepalive holdtime
```

To return to the default, use the `no timers bgp` command.

**Parameters**

- **keepalive**
  Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is **60 seconds**.

- **holdtime**
  Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

**Defaults** None

**Command Modes** EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048–ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048–ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---

**MBGP Commands**

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs). Dell Networking OS MBGP is implemented as per IETF RFC 1858.

BGPv4 is supported in the following:
**debug ip bgp dampening**

View information on routes being dampened.

**Syntax**

depth ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 unicast] dampening

To disable debugging, use the no debug ip bgp dampening command.

**Parameters**

- **vrf vrf-name**: Enter the keyword vrf followed by the name of the VRF to view information on dampened routes corresponding to that VRF.
- **ipv4 multicast**: (OPTIONAL) Enter the keyword ipv4 followed by the keyword multicast to view dampened-route information related only to ipv4 multicast routes.
- **ipv4 unicast**: (OPTIONAL) Enter the keyword ipv4 followed by the keyword unicast to view dampened-route information related only to ipv4 unicast routes.
- **ipv6 unicast**: (OPTIONAL) Enter the keyword ipv4 followed by the keyword unicast to view dampened-route information related only to ipv6 unicast routes.

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced IPv6 MGBP support for the E-Series.</td>
</tr>
</tbody>
</table>
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 BGP

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

⚠️ **CAUTION**: Dell Networking recommends not changing the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

Related Commands

- **router bgp** — enter ROUTER mode on the switch.
show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
dampened-paths
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
- `ipv4 multicast` (OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
- `ipv4 unicast` (OPTIONAL) Enter the keywords `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
- `ipv6 unicast` (OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

```
Version     Description
---------    -----------
9.8(1.0)     Introduced on the Z9100-ON.
9.8(0.0P5)   Introduced on the S4048-ON.
9.8(0.0P2)   Introduced on the S3048-ON.
9.7(0.0)     Added the ipv4 multicast and ipv6 unicast parameters.
9.4(0.0)     Added support for VRF.
9.2(1.0)     Introduced on the Z9500.
9.0.2.0      Introduced on the S6000.
8.3.19.0     Introduced on the S4820T.
8.3.11.1     Introduced on the Z9000.
8.3.7.0      Introduced on the S4810.
7.8.1.0      Introduced on the S-Series.
7.7.1.0      Introduced on the C-Series.
```

Usage Information

Usage Information

To determine a BGP session flap, both a route-down event and a subsequent route-up event corresponding to a single route are considered. As a result, a flap event is penalized only one time during the route-down event. The subsequent route-up event corresponding to the same route is not considered as a flap and is not penalized.
The history paths that the `show ip bgp` command displays contain only the prefix and the next-hop information. The next-hop information shows the ip address of the neighbor. It does not show the actual next-hop details. The following describes the `show ip bgp damp` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Displays the network ID to which the route is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>Displays the IP address of the neighbor advertising the dampened route.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Displays the hour:minutes:seconds until the dampened route is available.</td>
</tr>
<tr>
<td>Path</td>
<td>Lists all the ASs the dampened route passed through to reach the destination network.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip bgp dampened-paths
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
     n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network            From            Reuse     Path
      d   55.0.0.0/24      172.16.0.2             00:36:23      200

Dell#
```

**BGP Extended Communities (RFC 4360)**

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute. BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new “Type” field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

**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**

- **as4 ASN4:NN** Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
- **ASN:NNNN** Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
### Command: `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]}
```

#### Parameters
- **as4 ASN4:NN**: Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).

#### Usage Information
If the `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` — set the extended community site-of-origin in the route-map.

---

### Command: `IPADDR:NN`  
Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

### Command: `additive`  
(Optional) Enter the keyword `additive` to add to the existing extended community.

### Command: `non-trans`  
(Optional) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

#### Defaults
`none`

#### Command Modes
- **ROUTE MAP (config-route-map)**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z-9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---
**ASN:NNNN**
Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).

**IPADDR:NN**
Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

**non-trans**
(Optional) Enter the keywords non-trans to indicate a non-transitive BGP extended community.

**Defaults**
one

**Command Modes**
ROUTE MAP (config-route-map)

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

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.319.0 | Introduced on the S4820T.
8.311.1 | Introduced on the Z9000.
8.37.0 | Introduced on the S4810.
7.81.0 | Introduced on the S-Series.
7.71.0 | Introduced on the C-Series.
7.61.0 | Introduced on the E-Series.

**Usage Information**
If the set community rt and soo are in the same route-map entry, the behavior defines as:

- If the rt option comes before soo, with or without the additive option, soo overrides the communities rt sets.
- If the rt option comes after soo, without the additive option, rt overrides the communities soo sets.
- If the rt with the additive option comes after soo, rt adds the communities soo sets.

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

## Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>Version 7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

## Usage Information

The following describes the `show ip bgp paths extcommunity` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Displays the internal address where the path attribute is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Displays the hash bucket where the path attribute is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Displays the number of BGP routes using these extended communities.</td>
</tr>
<tr>
<td>Community</td>
<td>Displays the extended community attributes in this BGP path.</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show ip bgp paths extcommunity
Total 1 Extended Communities

Address     Hash  Refcount Extended Community
  0x41d57024  12272 1        RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

Dell#
```

### show ip extcommunity-list

Display the IP extended community list.

**Syntax**

```
show ip extcommunity-list [word]
```

**Parameters**

| word | Enter the name of the extended community list you want to view. |

**Command Modes**

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

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show ip extcommunity-list test
ip extcommunity-list test
deny RT:1234:12
permit regexp 123
deny regexp 234
deny regexp 123
Dell#
```

## IPv6 BGP Commands

IPv6 border gateway protocol (IPv6 BGP) is supported on the platform.

BGP is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

### 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

- **as-number**
  - 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).
- **peer-group name**
  - Clear and reapply policies for all BGP routers in the specified peer group.
- **ipv4-neighbor-addr** | **ipv6-neighbor-addr**
  - Clear and reapply policies for a neighbor.
- **ipv6 unicast**
  - Clear and reapply policies for all IPv6 unicast routes.

---

436  | Border Gateway Protocol
Reapply only inbound policies.

| NOTE | If you enter soft, without an in or out option, both inbound and outbound policies are reset. |

Reapply only outbound policies.

| NOTE | If you enter soft, without an in or out option, both inbound and outbound policies are reset. |

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv6 unicast routes.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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

**Command History**

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

**Command History**

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

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv6 unicast routes.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

**Syntax**

```plaintext
eighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

**Parameters**

- `ipv4-address | ipv6-address`  
Enter the IP address of the neighbor for which you want to start storing inbound routing updates.

- `peer-group-name`  
Enter the name of the peer group for which you want to start storing inbound routing updates.

**Defaults**

Disabled.

**Command Modes**

ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv4 multicast and IPv4 unicast address families.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**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.

**show ipv6 prefix-list**

Displays the specified IPv6 prefix list.

**Syntax**

```plaintext
show ipv6 prefix-list detail {prefix-list name} | summary
```

**Parameters**

- `detail`  
Display a detailed description of the selected IPv6 prefix list.
**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**

- **ipv6-address prefix-length**
  
  (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.
  
  **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

- **summary**
  
  Display a summary of RPF routes.

**Command Modes**

EXEC

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Content Addressable Memory (CAM)

You can use content addressable memory (CAM) commands to configure the amount of memory allocated to CAM memory partitions.

**NOTE:** Not all CAM commands are supported on all platforms. Be sure to note the platform when looking for a command.

**WARNING:** If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance.

### CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control lists (ACLs) (when IPv6 is not employed).
- Hash multi-protocol label switching (MPLS) packets based on source and destination IP addresses for link aggregation groups (LAGs).
- Hash based on bidirectional flow for LAGs.
- Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

### Important Points to Remember

- Dell Networking OS supports CAM allocations on the C-Series and S-Series.
- All line cards within a single system must have the same CAM profile (including CAM sub-region configurations); this profile must match the system CAM profile (the profile on the primary route processor module [RPM]).
- Dell Networking OS automatically reconfigures the CAM profile on line cards and the secondary RPM to match the system CAM profile by saving the correct profile on the card and then rebooting it.
- The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with port range options might require more than one CAM entry.
- After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

### CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control lists (ACLs) (when IPv6 is not employed).
- Hash multi-protocol label switching (MPLS) packets based on source and destination IP addresses for link aggregation groups (LAGs).
• Hash based on bidirectional flow for LAGs.
• Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

**Important Points to Remember**

• Dell Networking OS supports CAM allocations on the C-Series and S-Series.
• All line cards within a single system must have the same CAM profile (including CAM sub-region configurations); this profile must match the system CAM profile (the profile on the primary route processor module [RPM]).
• Dell Networking OS automatically reconfigures the CAM profile on line cards and the secondary RPM to match the system CAM profile by saving the correct profile on the card and then rebooting it.
• The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
• When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with port range options might require more than one CAM entry.
• After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
• You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

**cam-acl (Configuration)**

Select the default CAM allocation settings or reconfigure a new CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, OpenFlow, and Policy-based Routing (PBR).

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos number l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos number] ecfmacl number [nlbclusteracl number] ipv4pbr number [openflow number | fcoe number] [iscsiopticl number] [vrfv4acl number]}
```

**Parameters**

- **default**
  Use the default CAM profile settings and set the CAM as follows:
  - L2Acl : 6
  - IPv4Acl : 4
  - IPv6Acl : 0
  - IPv4Qos : 2
  - L2Qos : 1
  - L2PT : 0
  - IpMacAcl : 0
  - VmanQos : 0
  - VmanDualQos : 0
  - EcfmAcl : 0
  - nlbclusteracl : 0
  - FcoeAcl : 0
  - iscsiOptAcl : 0
  - ipv4pbr : 0
  - vrfv4Acl : 0
  - Openflow : 0
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>l2acl number</strong></td>
<td>Enter the keyword <code>l2acl</code> and then the number of l2acl blocks. The range is from 1 to 8.</td>
</tr>
<tr>
<td><strong>ipv4acl number</strong></td>
<td>Enter the keyword <code>ipv4acl</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.</td>
</tr>
<tr>
<td><strong>ipv6acl number</strong></td>
<td>Enter the keyword <code>ipv6acl</code> and then the number of FP blocks for IPv6. The range is from 0 to 4.</td>
</tr>
<tr>
<td><strong>ipv4qos number</strong></td>
<td>Enter the keyword <code>ipv4qos</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.</td>
</tr>
<tr>
<td><strong>l2qos number</strong></td>
<td>Enter the keyword <code>l2qos</code> and then the number of FP blocks for l2 qos. The range is from 1 to 8.</td>
</tr>
<tr>
<td><strong>l2pt number</strong></td>
<td>Enter the keyword <code>l2pt</code> and then the number of FP blocks for l2 protocol tunnelling. The range is from 0 to 1.</td>
</tr>
<tr>
<td><strong>ipmacacl number</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>ecfmacl number</strong></td>
<td>Enter the keyword <code>ecfmacl</code> and then the number of FP blocks for ECFM ACL. The range is from 0 to 5.</td>
</tr>
<tr>
<td><strong>nlbclusteracl number</strong></td>
<td>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 8 NLB ARP entries reserved for internal functionality.</td>
</tr>
</tbody>
</table>

**NOTE:** When you reconfigure CAM allocation, use the `nlbclusteracl number` command to change the number of NLB ARP entries. The range is from 0 to 2. The default value is 0. At the default value of 0, eight NLB ARP entries are available for use. This platform supports up to 512 CAM entries. Select 1 to configure 256 entries. Select 2 to configure 512 entries. Even though you can perform CAM carving to allocate the maximum number of NLB entries, Dell Networking recommends that you use a maximum of 64 NLB ARP entries.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vman-qos</strong></td>
<td>Enter the keyword <code>vman-qos</code> and then the number of FP blocks for VMAN GoS. The range is from 0 to 6.</td>
</tr>
<tr>
<td><strong>vman-dual-qos number</strong></td>
<td>Enter the keyword <code>vman-dual-qos</code> and then the number of FP blocks for VMAN dual GoS. The range is from 0 to 4.</td>
</tr>
<tr>
<td><strong>ipv4pbr number</strong></td>
<td>Enter the keyword <code>ipv4pbr</code> and then the number of FP blocks for ipv4pbr ACL. The range is from 0 to 8.</td>
</tr>
<tr>
<td><strong>Openflow number</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>fcoeacl number</strong></td>
<td>Enter the keyword <code>fcoeacl</code> and then the number of FP blocks for FCOE ACL. The range is from 0 to 6.</td>
</tr>
<tr>
<td><strong>iscsioptacl number</strong></td>
<td>Enter the keyword <code>iscsioptacl</code> and then the number of FP blocks for iSCSI optimization ACL. The range is from 0 to 2.</td>
</tr>
</tbody>
</table>

Allocate space to each CAM region.

Enter 4 or 8 for the number of OpenFlow FP blocks.

- 4: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality)
- 8: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality)
The fcoe range is 0–6 groups. Each group has 128 entries; the value given must be an even number. This information is stored in the NVRAM and is effective after rebooting the switch.

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added the nlbcluster ACL keyword. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for PBR and VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Added support for fcoe.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Added support for OpenFlow.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.2</td>
<td>Clarified block information for the S4810.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the keywords ecfmacl, vman-qos, and vman-dual-qos.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Save the new CAM settings to the startup-config (write-mem or copy run start) then reload the system for the new settings to take effect.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated. Only 13 number of blocks can be configured by the user.

The ipv6acl allocation must be a factor of 2.

If allocation values are not entered for the CAM regions, the value is 0.

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

---

**Content Addressable Memory (CAM)**

445
cam-acl-egress

Allocate CAM for egress ACLs.

Syntax

```
cam-acl-egress default | l2acl number ipv4acl number ipv6acl number
```

Parameters

- `default`:
  Reset egress CAM ACL entries to default settings.

- `l2acl number`:
  Allocate space to each CAM region. The total space allocated must equal 4. The ipv6acl range must be a factor of 2.

Command Modes

- **CONFIGURATION**

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Syntax

```
cam-optimization [qos]
```

Parameters

- `qos`:
  Optimize CAM usage for QoS.

Defaults

Disabled.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

When you enable this command, if a Policy Map containing classification rules (ACL and/or dscp/ ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy is written (only one FP entry is used).

**NOTE:** An ACL itself may still require more that a single FP entry, regardless of the number of interfaces. For more information, refer to the “IP Access Control Lists”, “Prefix Lists”, and “Route-map” sections in the Dell Networking OS Configuration Guide.

**show cam-acl**

Display the details of the CAM profiles on the chassis and all stack units.

**Syntax**

```
show cam-acl
```

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

The display reflects the settings implemented with the `cam-acl` command.

### Example

Dell# show cam-acl

```
-- Chassis Cam ACL --
Current Settings (in block sizes)
1 block = 256 entries

L2Acl   :  2
IPv4Acl :  4
IPv6Acl :  4
IPv4Qos :  2
L2Qos   :  1
L2PT    :  0
IpMacAcl:  0
VmanQos :  0
EcfmAcl :  0
FcoeAcl :  0
iscsiOptAcl :  0
ipv4pbr  :  0
vrffv4Acl:  0
Openflow :  0
fedgovacl:  0
nlbclusteracl:  0

-- stack-unit 1 --
Current Settings (in block sizes)
1 block = 256 entries

L2Acl   :  2
IPv4Acl :  4
IPv6Acl :  4
IPv4Qos :  2
L2Qos   :  1
L2PT    :  0
IpMacAcl:  0
VmanQos :  0
EcfmAcl :  0
FcoeAcl :  0
iscsiOptAcl :  0
ipv4pbr  :  0
vrffv4Acl:  0
Openflow :  0
fedgovacl:  0
nlbclusteracl:  0

-- stack-unit 3 --
Current Settings (in block sizes)
1 block = 256 entries

L2Acl   :  2
IPv4Acl :  4
IPv6Acl :  4
IPv4Qos :  2
L2Qos   :  1
L2PT    :  0
IpMacAcl:  0
VmanQos :  0
EcfmAcl :  0
FcoeAcl :  0
iscsiOptAcl :  0
ipv4pbr  :  0
vrffv4Acl:  0
Openflow :  0
fedgovacl:  0
```
**test cam-usage**

Verify that enough CAM space is available for the IPv6 ACLs you have created.

**Syntax**

test cam-usage service-policy input input policy name stack-unit {number | all}

**Parameters**

- **policy-map name**: Enter the name of the policy-map to verify. Maximum is 32 characters.
- **number**: Enter all to get information for all the stack-units or enter the stack-unit number to get information for a specific stack-unit.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs.

GoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.

The following describes the `test cam-usage` command shown in the following example.

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack-Unit</td>
<td>Lists the stack unit or units that are checked. Entering all shows the status for all stacks.</td>
</tr>
<tr>
<td>Term</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for stack-units and port-pipes in the chassis. The port set value is from 0 to 0.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>Shows the CAM profile of the CAM.</td>
</tr>
<tr>
<td>Available CAM</td>
<td>Identifies the amount of CAM space remaining for that profile.</td>
</tr>
<tr>
<td>Estimated CAM per Port</td>
<td>Estimates the amount of CAM space the listed policy will require.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether or not the policy will be allowed in the CAM.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# test cam-usage service-policy input In stack-unit all
Stack-Unit|Portpipe|CAM Partition|Available CAM|Estimated CAM per Port|Status
-----------------------------------------------------------------------------------------------
  1 | 0  | IPv4Flow  | 102 | 0| Allowed
Dell#
```

```
Dell# test cam-usage service-policy input In stack-unit 1 port-set 0
Stack-Unit|Portpipe|CAM Partition|Available CAM|Estimated CAM per Port|Status
-----------------------------------------------------------------------------------------------
  1 | 0  | IPv4Flow  | 102 | 0| Allowed
Dell#
```
Control Plane Policing (CoPP)

Control plane policing (CoPP) uses access control list (ACL) rules and quality of service (QoS) policies to create filters for a system’s control plane. The CoPP filters prevent traffic that is not identified as legitimate from reaching the control plane, and rate-limit traffic to an acceptable level.

Topics:
- control-plane-cpuqos
- service-policy rate-limit-cpu-queues
- service-policy rate-limit-protocols
- ip unknown-unicast
- ipv6 unknown-unicast
- 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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(8.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
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

Command History

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

    Version     Description
    9.8(1.0)     Introduced on the Z9100-ON.
    9.8(0.0P5)   Introduced on the S4048-ON.
    9.8(0.0P2)   Introduced on the S3048-ON.
    9.7(0.0)     Introduced on the S6000-ON.
    9.0.2.0      Introduced on the S6000.
    8.3.19.0     Introduced on the S4820T.
    8.3.11.1     Introduced on the Z9000.
    8.3.8.0      Introduced on the S4810.

Usage Information

    Create a policy-map by associating a queue number with the qos-policy.

    Create QoS policies prior to enabling this command.

    For CoPP, use the keyword cpu-qos when creating qos-policy-input.

Related Commands

    - qos-policy-input — create a QoS input policy map.
    - policy-map-input — create an input policy map.

service-policy rate-limit-protocols

Apply a policy for the system to rate limit control protocols on a per-protocol basis.

Syntax

    service-policy rate-limit-protocols policy-name
Parameters

- **policy-name**: Enter the service-policy name, using a string up to 32 characters.

Defaults

Not configured.

Command Modes

CONTROL-PLANE-CPUQOS

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

For CoPP, use the keyword cpu-qos when creating qos-policy-input.

Related Commands

- `ip access-list extended` — creates an extended IP ACL.
- `mac access-list extended` — creates an extended MAC ACL.
- `qos-policy-input` — creates a QoS input policy map.
- `class-map` — creates a QoS class map.
- `policy-map-input` — creates an input policy map.

ip unknown-unicast

Enable IPv4 catch-all route.

Syntax

```plaintext
ip unknown-unicast [vrf vrf-name]
```

To remove the IPv4 catch-all route (0.0.0.0/0) from the LPM route forwarding table in hardware which gets added as a default configuration after the initialization of FIB Agent module, use the no ip unknown-unicast command.

Defaults

None
Parameters

**vrf vrf-name**  
(Optional) Enter the keyword vrf followed by the name of the VRF to enable catch-all routes corresponding to that VRF.

Command Modes

**CONFIGURATION**

Command History

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

### Version Description

- **9.8(1.0)**  
  Introduced on the Z9100-ON.

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

- **9.8(0.0P2)**  
  Introduced on the S3048-ON.

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

- **9.4(0.0)**  
  Introduced on the S-Series.

Usage Information

Use this command to add the IPv4 catch-all route (0.0.0.0/0) in the LPM route forwarding table if it was deleted using the `no ip unknown-unicast` command previously. This will be the default configuration after reload.

### ipv6 unknown-unicast

Disable soft forwarding of unknown IPv6 destination packets.

Syntax

```plaintext
[no] ipv6 unknown-unicast
```

Defaults

Soft forwarding is 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

- **9.10(0.0)**  
  Introduced on the S6100-ON.

- **9.8(1.0)**  
  Introduced on the Z9100-ON.

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

- **9.8(0.0P2)**  
  Introduced on the S3048-ON.

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

- **9.4(0.0)**  
  Introduced on the S-Series.

Usage Information

All the default catch-all entries in the longest prefix match (LPM) table collect and transmit all unresolved IPv6 packets to the CPU, even if they are destined for unknown destinations.
show cpu-queue rate cp

Display the rates for each CPU queue.

Syntax

show cpu-queue rate cp

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0)Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.8.0 Introduced on the S4810.

Usage Information

This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

Example

Dell#show cpu-queue rate cp

<table>
<thead>
<tr>
<th>Service-Queue</th>
<th>Rate (PPS)</th>
<th>Burst (Packets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q0</td>
<td>600</td>
<td>512</td>
</tr>
<tr>
<td>Q1</td>
<td>1000</td>
<td>50</td>
</tr>
<tr>
<td>Q2</td>
<td>300</td>
<td>50</td>
</tr>
<tr>
<td>Q3</td>
<td>1300</td>
<td>50</td>
</tr>
<tr>
<td>Q4</td>
<td>2000</td>
<td>50</td>
</tr>
<tr>
<td>Q5</td>
<td>400</td>
<td>50</td>
</tr>
<tr>
<td>Q6</td>
<td>400</td>
<td>50</td>
</tr>
<tr>
<td>Q7</td>
<td>400</td>
<td>50</td>
</tr>
<tr>
<td>Q8</td>
<td>600</td>
<td>50</td>
</tr>
<tr>
<td>Q9</td>
<td>600</td>
<td>50</td>
</tr>
<tr>
<td>Q10</td>
<td>600</td>
<td>50</td>
</tr>
<tr>
<td>Q11</td>
<td>300</td>
<td>50</td>
</tr>
</tbody>
</table>

Dell#
show ip protocol-queue-mapping

Display the queue mapping for each configured protocol.

Syntax

```
show ip protocol-queue-mapping
```

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(8.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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       any     _       Q6    _       _
ICMPV6 RA any      any       any     _       Q6    _       _
ICMPV6 NS any      any       any     _       Q5    _       _
ICMPV6 RS any      any       any     _       Q5    _       _
ICMPV6 any      any       any     _       Q6    _       _
VRRPV6 any      any       any     _       Q10   _      _
OSPFV3 any      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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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#
Debugging and Diagnostics

The basic debugging and diagnostic commands are supported by the Dell Networking OS.

Topics:
- Diagnostics and Monitoring Commands
- Offline Diagnostic Commands
- Hardware Commands

Diagnostics and Monitoring Commands

The following section describes the diagnostics and monitoring commands. For similar commands, refer to the Control and Monitoring chapter.

logging coredump stack-unit

Enable coredump on a stack.

Syntax

logging coredump stack-unit {stack-unit-number | all}

Parameters

- stack-unit stack-unit-number: Enter the stack-unit id to enable coredump in a particular stack-unit.
- all: Enable coredump on all stack-unit.

Defaults

Disabled by default on customer builds.

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Usage Information

The Kernel core dump can be large and may take up to 5 to 30 minutes to upload. Dell Networking OS does not overwrite application core dumps so you should delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted. On the S-Series, if the FTP server is not reachable, the application coredump is aborted. Dell Networking OS completes the coredump process and wait until the upload is complete before rebooting the system.

Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, Dell Networking OS results are saved as a text file (TestReport-SU-X.txt) in the flash directory. This show file command is available only on master and standby.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected to via a stacking link.
- The system stores the diagnostic results in the flash directory (TestReport-SU-X.txt). The system displays the following message after the diagnostic test is over.

  05:37:17 : Diagnostic test results are stored on file: flash:/TestReport-SU-1.txt
  05:37:22: %S3048-ON:1 %DIAGAGT-6-DA_DIAG_DONE: Diags finished on stack-unit 1

- Diagnostics only test connectivity, not the entire data path.


diag stack-unit

Run offline diagnostics on a stack unit.

Syntax

diag stack-unit number [alllevels | level0 | level1 | level2] verbose [testname | no-reboot]

Parameters

- **number**: Enter the stack-unit id.
- **alllevels**: Enter the keyword alllevels to run the complete set of offline diagnostic tests.
- **level0**: Enter the keyword level0 to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
- **level1**: Enter the keyword level1 to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, stack ports are shut down automatically.
- **level2**: Enter the keyword level2 to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations. To test 10G links, physically remove the unit from the stack.
verbose

Enter the keyword `verbose` to run the diagnostic in Verbose mode. Verbose mode gives more information in the output than Standard mode.

testname

Enter the keyword `testname` to run a specific test case. Enclose the test case name in double quotes (" "). For example: `diag stack-unit 1 level1 testname "first"`. You can use this option only for interactive tests.

no-reboot

Enter the keyword `no-reboot` to prevent the system from rebooting after the test. To bring the stack unit to online state, use the `online stack-unit stack-unit-number` command.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced the <code>verbose</code> option.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**offline stack-unit**

Place a stack unit in the offline state.

**Syntax**

`offline stack-unit number`

**Parameters**

- `number` Enter the stack-unit id.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
### online stack-unit

Place a stack unit in the online state.

**Syntax**

```
online stack-unit number
```

**Parameters**

- **number**
  
Enter the stack-unit number.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

#### Version Description

- **9.8(1.0)**  
  Introduced on the Z9100–ON.

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

- **9.8(0.0P2)**  
  Introduced on the S3048-ON.

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

- **9.0.2.0**  
  Introduced on the S6000.

- **8.3.19.0**  
  Introduced on the S4820T.

- **8.3.11.1**  
  Introduced on the Z9000.

- **8.3.7.0**  
  Introduced on the S4810.

- **8.2.1.0**  
  Added a warning message to the off-line diagnostic.

- **7.7.1.0**  
  Introduced on the S-Series.

### Usage Information

You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

Warning: Diagnostic execution will cause stack-unit to reboot after completion of diags.

Proceed with Offline-Diags [confirm yes/no]:y
Usage Information

You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This reboot is an automatic process. A warning message appears when the offline stack-unit command is implemented.

Warning - Diagnostic execution will cause stack-unit to reboot after completion of diags.

Proceed with Offline-Diags [confirm yes/no]:y

Hardware Commands

These commands display information from a hardware sub-component or ASIC.

clear hardware stack-unit

Clear statistics from selected hardware components.

Syntax

clear hardware stack-unit id {counters | cpu {data-plane statistics | i2c statistics | management statistics | party-bus statistics | sata-interface statistics} | unit number counters | stack-port stack-port-number}

Parameters

stack-unit id

Enter the keywords stack-unit then a number to select a particular stack member and then enter one of the following command options to clear a specific collection of data. The range is from 1 to 6.

counters

Enter the keyword counters to clear the counters on the selected stack member.

cpu data-plane statistics

Enter the keywords cpu data-plane statistics to clear the data plane statistics.

cpu i2c statistics

Enter the keywords cpu i2c statistics to clear the i2c devices statistics.

cpu party-bus statistics

Enter the keywords cpu party-bus statistics to clear the management statistics.

cpu sata-interface statistics

Enter the keywords cpu sata-interface statistics to clear the sata interface statistics.

stack-port

Enter the keywords stack-port then the port number of the stacking port to clear the statistics of the particular stacking port. The range is from 1 to 52.

Defaults

None

Command Modes

EXEC Privilege

Command History

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

Version Description

9.8(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.
clear hardware system-flow

Clear system-flow statistics from selected hardware components.

Syntax:
```
clear hardware system-flow layer2 stack-unit number port-set 0-0 counters
```

Parameters:
- **stack-unit number**: Enter the keywords stack-unit then a number to select a particular stack member and then enter one of the following command options to clear a specific collection of data.
- **port-set 0-0 counters**: Enter the keywords port-set along with a port-pipe number, then the keyword counters to clear the system-flow counters on the selected port-pipe. The range is from 0 to 0.

Defaults:
None

Command Modes:
EXEC Privilege

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

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.0 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.

Related Commands:
- **show hardware stack-unit** — display the data plane or management plane input and output statistics of the designated component of the designated stack member.
clear hardware vlan-counters

Clear VLAN statistics.

Syntax

clear hardware vlan-counters vlan-id

Parameters

vlan-id Enter the interface VLAN number. The range is from 1 to 4094.

Defaults
None

Command Modes
EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced this command.</td>
</tr>
</tbody>
</table>

hardware watchdog

To trigger a reboot and restart the system, set the watchdog timer.

Syntax

hardware watchdog stack-unit {stack-unit-number | all}

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
show hardware mac

Display MAC ACL entries for the specified stack-unit, port-pipe and pipeline ID.

Syntax

```
show hardware mac {eg-acl | in-acl} stack-unit id port-set 0–0
```

Parameters

- `eg-acl | in-acl` Enter either the keyword `eg-acl` or the keyword `in-acl` to select between ingress or egress ACL data.
- `stack-unit id` Enter the keyword `stack-unit` to select the stack unit ID.
- `port-set 0–0` Enter the keywords `port-set` with a port-pipe number to display the MAC ACL entries for the specified port-pipe number. The range is from 0 to 0.

Defaults

None

Command Modes

EXEC Privilege

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.

Usage Information

The unit numbers given are internal port numbers.

show hardware ip

Display ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware layer3 {acl | qos} stack-unit number port-set 0–0
```

Parameters

- `acl | qos` Enter either the keyword `acl` or the keyword `qos` to select between ACL or QoS data.
- `stack-unit number` Enter the keywords `stack-unit` then a number to select a stack ID.
- `port-set 0–0` Enter the keyword `port-set` with a port-pipe number. The range is from 0 to 0.
show hardware stack-unit

Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

Syntax

```
stack-unit stack-unit-number {cpu data-plane statistics | cpu management statistics | [ drops [unit number | fpga register | party-bus statistics | stack-port | ti-monitor | unit 0-1 {counters | details | port-stats [detail] | register}}
```

Parameters

- `stack-unit stack-unit-number (command-option)`: Enter the keywords `stack-unit` to select a particular stack member and then enter one of the following command options to display a collection of data based on the option entered. The range is from 1 to 6.
- `cpu data-plane statistics`: Enter the keywords `cpu data-plane statistics` then the keywords `stack port` and its number, from 1 to 52 to display the data plane statistics, which shows the High Gig (Higig) port raw input/output counter statistics to which the stacking module is connected.
- `cpu management statistics`: Enter the keywords `cpu management statistics` to display the counters of the management port.
- `cpu party-bus statistics`: Enter the keywords `cpu party-bus statistics`, to display the Management plane input/output counter statistics of the pseudo party bus interface.
- `cpu sata-interface statistics`: Enter the keywords `cpu sata-interface statistics` to display the sata interface error counter statistics.
- `drops [unit unit-number]`: Enter the keyword `drops` to display internal drops on the selected stack member. Enter the optional keyword `unit unit-number` to display the internal drop counters of the specified port pipe.
- `fpga register`: Enter the keyword to display the register value of the fpga register.
Enter the keyword `unit` then a number and then enter one of the keywords to troubleshoot errors on the selected port-pipe and to give status on why a port is not coming up to register level.

### TI monitor
Enter the unit keyword to show information regarding the TI register.

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Replaced the keyword <code>port</code> with <code>interface</code>.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Modified the <code>drops</code> keyword range, unit keyword range and added the <code>buffer</code> and <code>cpu management statistics</code> options.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.5</td>
<td>Added i2c statistics and sata-interfaces statistics.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Added user port information.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Example (Data-Plane)**

```
Dell# show hardware stack-unit 1 cpu data-plane statistics
Input Statistics:
  1856 packets, 338262 bytes
  141 64-byte pkts, 1248 over 64-byte pkts, 11 over 127-byte pkts
  222 over 255-byte pkts, 236 over 511-byte pkts, 0 over 1023-byte pkts
  919 Multicasts, 430 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded

Output Statistics:
  325 packets, 27629 bytes, 0 underruns
  9 64-byte pkts, 310 over 64-byte pkts, 1 over 127-byte pkts
  1 over 255-byte pkts, 2 over 511-byte pkts, 2 over 1023-byte pkts
  0 Multicasts, 3 Broadcasts, 322 Unicasts
  0 throttles, 0 discarded, 0 collisions

Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec
  Output 00.00 Mbits/sec
```

Dell#
Example (Party-Bus)  
Dell# show hardware stack-unit 1 cpu party-bus statistics  
Input Statistics:  
0 packets, 0 bytes  
0 dropped, 0 errors  
Output Statistics:  
0 packets, 0 bytes  
0 errors

Example (Drops Unit)  
Dell# sh hard stack-unit 1 drops unit 0  
PortNumber Ingress Drops IngMac Drops Total Mmu Drops  
1 0 0 0 0  
2 0 0 0 0  
3 0 0 0 0  
4 0 0 0 0  
EqMac Drops Egress Drops  
0 0 0 0  
0 0 0 0  
0 0 0 0  
Dell#

Example (Port-Stats)  
Dell# show hardware stack-unit 1 unit 0 port-stats  
ena/ speed/ link auto STP  
port link duplex scan neg? state pause discrd ops face frame back  
ge0 down - SW Yes Block Untag FA SGMII 1554  
ge1 !ena - SW Yes Block Tag FA SGMII 1554  
ge2 !ena - SW Yes Block Tag FA SGMII 1554  
ge3 !ena - SW Yes Forward Tag FA SGMII 1554  
ge4 !ena - SW Yes Forward Tag F SGMII 1554  
ge5 !ena - SW Yes Forward Tag F SGMII 1554  
ge6 !ena - SW Yes Forward Tag F SGMII 1554  
ge7 !ena - SW Yes Forward Tag F SGMII 1554  
ge8 !ena - SW Yes Forward Tag F SGMII 1554  
ge9 !ena - SW Yes Forward Tag F SGMII 1554  
ge10 !ena - SW Yes Forward Tag F SGMII 9252  
ge11 !ena - SW Yes Forward Tag F SGMII 9252  
ge12 !ena - SW Yes Forward Tag F SGMII 9252  
ge13 !ena - SW Yes Forward Tag F SGMII 9252  
ge14 !ena - SW Yes Forward Tag F SGMII 9252  
ge15 !ena - SW Yes Forward Tag F SGMII 9252  
ge16 !ena - SW Yes Forward Tag F SGMII 9252  
ge17 !ena - SW Yes Forward Tag F SGMII 9252  
ge18 !ena - SW Yes Forward Tag F SGMII 9252  
ge19 !ena - SW Yes Forward Tag F SGMII 9252  
ge20 !ena - SW Yes Forward Tag F SGMII 9252  
ge21 !ena - SW Yes Forward Tag F SGMII 9252  
ge22 !ena - SW Yes Forward Tag F SGMII 9252  
ge23 !ena - SW Yes Forward Tag F SGMII 9252  

Example (Register)  
Dell# show hardware stack-unit 1 unit 1 register  
0x0068003c AGINGCTRMEMDEBUG.mmu0 = 0x00000000  
0x0068003d AGINGEXPMEMDEBUG.mmu0 = 0x00000000  
0x00680017 ASFCONFIG.mmu0 = 0x0000000e  
0x0060004c ASFPORTSPEED.ge0 = 0x00000000  
0x0060104c ASFPORTSPEED.ge1 = 0x00000000  
0x0060204c ASFPORTSPEED.ge2 = 0x00000000  
0x0060304c ASFPORTSPEED.ge3 = 0x00000000  
0x0060404c ASFPORTSPEED.ge4 = 0x00000000  
0x0060504c ASFPORTSPEED.ge5 = 0x00000000  
0x0060604c ASFPORTSPEED.ge6 = 0x00000000  
0x0060704c ASFPORTSPEED.ge7 = 0x00000000  
0x0060804c ASFPORTSPEED.ge8 = 0x00000000  
0x0060904c ASFPORTSPEED.ge9 = 0x00000000  
0x0060a04c ASFPORTSPEED.ge10 = 0x00000000  
0x0060b04c ASFPORTSPEED.ge11 = 0x00000000  
0x0060c04c ASFPORTSPEED.ge12 = 0x00000000  
0x0060d04c ASFPORTSPEED.ge13 = 0x00000000  
0x0060e04c ASFPORTSPEED.ge14 = 0x00000000  
0x0060f04c ASFPORTSPEED.ge15 = 0x00000000  
0x0061004c ASFPORTSPEED.ge16 = 0x00000000  
0x0061104c ASFPORTSPEED.ge17 = 0x00000000  
0x0061204c ASFPORTSPEED.ge18 = 0x00000000  

Debugging and Diagnostics
Example (Counters)

Dell# show hardware stack-unit 1 unit 0 counters
unit: 0 port: 1 (interface Gi 1/1)

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX - IPV4 L3 Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV4 L3 Routed Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV6 L3 Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV6 L3 Routed Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - Unicast Packet Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 64 Byte Frame Counter</td>
<td>336186</td>
</tr>
<tr>
<td>RX - 65 to 127 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 128 to 255 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 256 to 511 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 512 to 1023 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 1024 to 1518 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 1519 to 2047 Byte Good VLAN Frame Counter</td>
<td>0</td>
</tr>
</tbody>
</table>

---------------- output truncated ----------------!
<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX - 2048 to 4095 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 4096 to 9216 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Good Packet Counter</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Packet/Frame Counter</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Multicast Frame Counter</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Broadcast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Byte Counter</td>
<td>21515904</td>
</tr>
<tr>
<td>RX - Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Pause Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Oversized Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Jabber Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Double VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - RUNT Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - VLAN Tagged Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - Ingress Dropped Packet</td>
<td>0</td>
</tr>
<tr>
<td>RX - MTU Check Error Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 0</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 1</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 2</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 3</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 4</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 5</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 6</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 7</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 0</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Debug Counter 1</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Debug Counter 2</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 3</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 4</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 5</td>
<td>336186</td>
</tr>
<tr>
<td>RX - Debug Counter 6</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 7</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 8</td>
<td>0</td>
</tr>
<tr>
<td>TX - 64 Byte Frame Counter</td>
<td>166</td>
</tr>
<tr>
<td>TX - 65 to 127 Byte Frame Counter</td>
<td>112</td>
</tr>
<tr>
<td>TX - 128 to 255 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 256 to 511 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 512 to 1023 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 1024 to 1518 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 1519 to 1522 Byte Good VLAN Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 1519 to 2047 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 2048 to 4095 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 4096 to 9216 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Good Packet Counter</td>
<td>278</td>
</tr>
<tr>
<td>TX - Packet/Frame Counter</td>
<td>278</td>
</tr>
<tr>
<td>TX - Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Multicast Frame Counter</td>
<td>278</td>
</tr>
<tr>
<td>TX - Broadcast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Byte Counter</td>
<td>18688</td>
</tr>
<tr>
<td>TX - Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Pause Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Oversized Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Jabber Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Double VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - RUNT Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 0</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 1</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 2</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 3</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 4</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 5</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 6</td>
<td>0</td>
</tr>
<tr>
<td>TX - PFC Frame Priority 7</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 0</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 1</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 2</td>
<td>0</td>
</tr>
<tr>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>TX - Debug Counter 3</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 4</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 5</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 6</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 7</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 8</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 9</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 10</td>
<td>0</td>
</tr>
<tr>
<td>TX - Debug Counter 11</td>
<td>0</td>
</tr>
</tbody>
</table>

-----

unit: 0 port: 61 (interface Gi 1/60)

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX - IPV4 L3 Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV4 L3 Routed Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV6 L3 Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - IPV6 L3 Routed Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - Unicast Packet Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 64 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 65 to 127 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 128 to 255 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 256 to 511 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 512 to 1023 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 1024 to 1518 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 1519 to 1522 Byte Good VLAN Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 1519 to 2047 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 2048 to 4095 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - 4096 to 9216 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Good Packet Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Packet/Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Unicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Multicast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Broadcast Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Byte Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Pause Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Oversized Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Jabber Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Double VLAN Tag Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - RUNT Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - VLAN Tagged Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX - Ingress Dropped Packet</td>
<td>0</td>
</tr>
<tr>
<td>RX - MTU Check Error Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 0</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 1</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 2</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 3</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 4</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 5</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 6</td>
<td>0</td>
</tr>
<tr>
<td>RX - PFC Frame Priority 7</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 0</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 1</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 2</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 3</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 4</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 5</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 6</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 7</td>
<td>0</td>
</tr>
<tr>
<td>RX - Debug Counter 8</td>
<td>0</td>
</tr>
<tr>
<td>TX - 64 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 65 to 127 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 128 to 255 Byte Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX - 256 to 511 Byte Frame Counter</td>
<td>0</td>
</tr>
</tbody>
</table>
TX - 512 to 1023 Byte Frame Counter 0
TX - 1024 to 1518 Byte Frame Counter 0
TX - 1519 to 1522 Byte Good VLAN Frame Counter 0
TX - 1519 to 2047 Byte Frame Counter 0
TX - 2048 to 4095 Byte Frame Counter 0
TX - 4096 to 9216 Byte Frame Counter 0
TX - Good Packet Counter 0
TX - Packet/Frame Counter 0
TX - Unicast Frame Counter 0
TX - Multicast Frame Counter 0
TX - Broadcast Frame Counter 0
TX - Byte Counter 0
TX - Control Frame Counter 0
TX - Pause Control Frame Counter 0
TX - Oversized Frame Counter 0
TX - Jabber Counter 0
TX - VLAN Tag Frame Counter 0
TX - Double VLAN Tag Frame Counter 0
TX - RUNT Frame Counter 0
TX - Fragment Counter 0
TX - PFC Frame Priority 0 0
TX - PFC Frame Priority 1 0
TX - PFC Frame Priority 2 0
TX - PFC Frame Priority 3 0
TX - PFC Frame Priority 4 0
TX - PFC Frame Priority 5 0
TX - PFC Frame Priority 6 0
TX - PFC Frame Priority 7 0
TX - Debug Counter 0 0
TX - Debug Counter 1 0
TX - Debug Counter 2 0
TX - Debug Counter 3 0
TX - Debug Counter 4 0
TX - Debug Counter 5 0
TX - Debug Counter 6 0
TX - Debug Counter 7 0
TX - Debug Counter 8 0
TX - Debug Counter 9 0
TX - Debug Counter 10 0
TX - Debug Counter 11 0

Example (Details)
Dell# show hardware stack-unit 1 unit 1 details

********************************************************************************
The total no of FP & CSF Devices in the Card is 2
The total no of FP Devices in the Card is 2
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 24
The number of Hg ports in devices 0 is - 4
The CPU Port of the device is 28
The number of ports in device 1 is - 24
The number of Hg ports in devices 1 is - 4
The CPU Port of the device is 28
The staring unit no the SWF in the device is 0
********************************************************************************
The Current Link Status Is
Front End Link Status 0x000000000000400000000000
Front End Port Present Status 0x000000000000000000000000
Back Plane Link Status 0x00000000
********************************************************************************
Link Status of all the ports in the Device - 1
The linkStatus of Front End Port 0 is FALSE
The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 2 is FALSE
The linkStatus of Front End Port 3 is FALSE
The linkStatus of Front End Port 4 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 6 is FALSE
The linkStatus of Front End Port 7 is FALSE
The linkStatus of Front End Port 8 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 10 is FALSE
The linkStatus of Front End Port 11 is FALSE
The linkStatus of Front End Port 12 is FALSE
The linkStatus of Front End Port 13 is FALSE
The linkStatus of Front End Port 14 is FALSE
The linkStatus of Front End Port 15 is FALSE
The linkStatus of Front End Port 16 is FALSE
The linkStatus of Front End Port 17 is FALSE
The linkStatus of Front End Port 18 is FALSE
The linkStatus of Front End Port 19 is FALSE
The linkStatus of Front End Port 20 is FALSE
The linkStatus of Front End Port 21 is FALSE
The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is TRUE
The linkStatus of Hg Port 24 is TRUE
The linkStatus of Hg Port 25 is TRUE
The linkStatus of Hg Port 26 is FALSE
The linkStatus of Hg Port 27 is FALSE

!------------------ output truncated ---------------!

Example (Total-Buffer)

Dell# show hardware stack-unit 1 buffer total-buffer

----- Buffer Details for Stack-Unit 1 -----    
Total Buffers allocated per Stack-Unit 46080

Example displaying queue range

Dell# show hardware stack-unit 0 buffer unit 0 interface all queue 6 buffer-info

Buffer Stats for Front End Ports

----- Buffer Stats for Interface Gi 1/0 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/2 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/3 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/4 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/5 Queue 6 ----- 
Maximum Shared Limit: 7667 
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/6 Queue 6 ----- 
<output truncated for brevity>

Related Commands

- clear hardware system-flow — clear the statistics from selected hardware components.
- show interfaces stack-unit — display information on all interfaces on a specific S-Series stack member.
- show processes cpu (S-Series) — display the CPU usage information based on the processes running in an S-Series.
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
```

Parameters

- `interface interface` Enter any of the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- `priority-group` Enter the keyword `priority-group` followed by `id` for specific priority-group or keyword `all`.
- `queue` Enter the keyword `queue` followed by `id` for specific queue or keyword `all`.
- `buffer-info` To display total buffer information for the interface, enter the keywords `buffer-info`.

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9000, and Z9500.</td>
</tr>
</tbody>
</table>

Example displaying total-buffer information for the interface:

```
Dell# show hardware buffer interface gigabitethernet 1/1 buffer-info
----- Buffer Stats for Interface Gi 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 gigabitethernet 1/1 priority-group 0 buffer-info
----- Buffer stats for unit: 0 port: 1 (interface Gi 1/1) -----                       
PG# PRIORITIES ALLOTED (CELLS) COUNTER (CELLS)                                   
--------------------------------------- --------- --------- ----------- ----------- 
0 - 61440 0 STATIC 174 0 0 0
```
Example displaying queue range

Dell# show hardware buffer interface gigabitethernet 1/1 queue all buffer-info
----- Buffer Stats for Interface Gi 1/1 Queue 0 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 1 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 2 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 3 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 4 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 5 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 6 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 7 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 8 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 9 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 1/1 Queue 10 -----  
Maximum Shared Limit: 29514  
Default Packet Buffer allocate for the Queue: 8  
Used Packet Buffer: 0

----- Buffer Stats for Interface Gi 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

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 the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.

476 | Debugging and Diagnostics
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Defaults
None

Command Modes
- EXEC
- EXEC Privilege

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

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0) Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.

Example
Dell# show hardware counters interfac gigabitethernet 5/1
unit: 0 port: 2 (interface G1 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 - PFC Frame Priority 8                          0
RX - PFC Frame Priority 9                          0
RX - Debug Counter 0                               0
show hardware buffer-stats-snapshot

Displays buffer statistics tracking resource information for a specific interface.

Syntax

show hardware buffer-stats-snapshot resource interface interface {priority-group {id | all} | queue ucast {id | all} mcast {id | all} | all} [detail]

Parameters

interface interface Enter any of the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

queue Enter the keyword queue followed by all for displaying details of all queues, ucast queue-id or all for displaying Unicast queue details, and mcast queue-id or all for displaying Multicast queue details.

priority-group Enter the keyword priority-group followed by id for specific priority-group or keyword all.

Command Modes

EXEC

EXEC Privilege

Command History

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

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.
9.8(0.0) Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9000, Z9500.

Usage Information

<Interface><slot/port>-Queue ucast/mcast — Displays the total unicast/multicast buffer usage on per-port per-queue basis. For CPU port, counters for queues 0 to 11 displays and there is no differentiation between unicast and multicast queues.
show hardware stack-unit buffer-stats-snapshot (Total Buffer Information)

View the buffer statistics tracking resource information depending on the type of buffer information, such as device-level details, port-level counters, queue-based snapshots, or priority group-level snapshot in the egress and ingress direction of traffic.

Syntax

```
show hardware stack-unit <id> buffer-stats-snapshot unit <id> resource x
```

Parameters

- `stack-unit stack-unit-number` - Unique ID of the stack unit to select a particular stack member and then enter one of the following command options to display a collection of data based on the option entered.
- `buffer-stats-snapshot unit number` - Display the historical snapshot of buffer statistical values unit Enter the keyword `unit` along with a port-pipe number. The range is from 0 to 0.
- `buffer-info` - Buffer and traffic manager resources usage, where X can be one of the following:
  - All - Displays ingress and egress device, port, and queue snapshots
  - Interface all queue {all} - egress queue-level snapshot for both unicast and multicast packets
  - Interface all queue ucast {id | all} - egress queue-level snapshot for unicast packets only
  - Interface all queue mcast {id | all} - egress queue-level snapshot for multicast packets only
  - Interface all prio-group {id | all} - ingress priority-group level snapshot

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the keyword <code>interface all</code>.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Introduced on the S5000.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S6000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

Usage Information

The following information is displayed based on the buffer-info type, such as device-level details, queue-based snapshots, or priority group-level snapshot in the egress and ingress direction of traffic:

- Device-ingress – Displays total buffer accounting usage for the unit.
- Device-egress – Display total buffer usage for the unit, total multicast buffer usage for the unit and also on per-service-pool basis. Counters will be displayed for the 2 service-pools – one for normal traffic and other for DCB traffic.
When the buffer-stats-snapshot is disabled, the following informational message is displayed when you run the show command: %Info: Buffer-stats-snapshot feature is disabled.

Example

Dell# show hardware stack-unit 1 buffer-stats-snapshot unit 3 resource interface all queue mcast 3
Unit 1 unit: 3 port: 1 (interface Fo 1/144)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 5 (interface Fo 1/148)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 9 (interface Fo 1/152)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 13 (interface Fo 1/156)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 17 (interface Fo 1/160)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 21 (interface Fo 1/164)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 25 (interface Fo 1/168)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 29 (interface Fo 1/172)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 33 (interface Fo 1/176)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Unit 1 unit: 3 port: 37 (interface Fo 1/180)

<table>
<thead>
<tr>
<th>Q# TYPE</th>
<th>Q#</th>
<th>TOTAL BUFFERED CELLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAST</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax

```
show hardware system-flow stack-unit id port-set number [counters]
```

Parameters

- **stack-unit id**: Enter the keywords `stack-unit` to select a stack member ID.
- **port-set number [counters]**: Enter the keywords `port-set` with a port-pipe number. (OPTIONAL) Enter the keyword `counters` for the specified port-pipe.

Defaults

None

Command Modes

EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show hardware system-flow stack-unit 1 port-set 0 counters
-----------------------------------------------------------
<table>
<thead>
<tr>
<th>EntryId</th>
<th>Description</th>
<th>#HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2048</td>
<td>STP BPDU Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2047</td>
<td>LLDP BPDU Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2045</td>
<td>LACP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2044</td>
<td>GVRP traffic Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2043</td>
<td>ARP Reply Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2042</td>
<td>802.1x frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2041</td>
<td>VRRP frames Redirects</td>
<td>0</td>
</tr>
<tr>
<td>2040</td>
<td>GRAT ARP</td>
<td>0</td>
</tr>
<tr>
<td>2039</td>
<td>DROP Cases</td>
<td>0</td>
</tr>
<tr>
<td>2038</td>
<td>OSPF1 STUB</td>
<td>0</td>
</tr>
<tr>
<td>2037</td>
<td>OSPF2 STUB</td>
<td>0</td>
</tr>
<tr>
<td>2036</td>
<td>VRRP STUB</td>
<td>0</td>
</tr>
<tr>
<td>2035</td>
<td>L2_DST_HIT+BC MAC+VLAN 4095</td>
<td>0</td>
</tr>
<tr>
<td>2034</td>
<td>L2_DST_HIT+BC MAC</td>
<td>0</td>
</tr>
<tr>
<td>2033</td>
<td>Catch all</td>
<td>0</td>
</tr>
<tr>
<td>384</td>
<td>OSPF[224.0.0.5] Packets</td>
<td>0</td>
</tr>
<tr>
<td>383</td>
<td>OSPF[224.0.0.6] Packets</td>
<td>0</td>
</tr>
<tr>
<td>382</td>
<td>VRRP Packets</td>
<td>0</td>
</tr>
<tr>
<td>380</td>
<td>BCast L2_DST_HIT on VLAN 4095</td>
<td>0</td>
</tr>
<tr>
<td>379</td>
<td>BCAST L2_DST_HIT Packets</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show hardware vlan-counters

Display the hardware VLAN statistics.

Syntax

    show hardware vlan-counters vlan-id

Example

    param1=0(0x00),
    action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
    action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
    action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
    meter=NULL,
    counter={idx=1, mode=0x01, entries=1}

########### FP Entry for redirecting LACP traffic to CPU Port ###########

EID 2045: gid=1,
slice=15, slice_idx=0x02, prio=0x7fd, flags=0x82, Installed
tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 0180c200 00020000 00000000 00000000
, FPF4=0x00
MASK=0x00000000 00000000 00000000 ffffff 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 ffffffff ffff0000 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 00000000 00000000
, FPF4=0x00
MASK=0x00000000 00000000 00000000 00000000 0000806 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 -----------------!
Parameters

**vlan-id**
Enter the interface VLAN number. The range is from 1 to 4094.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced this command.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show hardware vlan-counters 1
Counters for vlanid: 1
------------------------
Total number of inpackets: 0
Total number of inbytes: 0
Total number of outpackets: 0
Total number of outbytes: 0
Dell#
```

Related Commands

- `clear hardware system-flow` — clear the statistics from selected hardware components.

**show hardware drops**

Displays internal drops on the specified interface or for a range of interface.

Syntax

```
show hardware drops interface interface
```

Parameters

- **drops**
Enter the keyword *drops* to display internal drops.

- **interface**
Enter any of the following keywords and the interface or interface range information:
  - For a 1-GigabitEthernet interface, enter the keyword *GigabitEthernet* then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword *TenGigabitEthernet* then the slot/port information.

Command Modes

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Removed the keywords stack-unit. Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Modified the drops keyword range, unit keyword range and added the buffer and cpu management statistics options.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.5</td>
<td>Added i2c statistics and sata-interfaces statistics.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Added user port information.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Example displaying internal drops for the specific interface:

```
Dell# show hardware drops interface gigabitethernet 2/1
Drops in Interface Gi 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 : 0
  (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
Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on the configuration policies the network administrators determine.

Topics:
- Commands to Configure the System to be a DHCP Server
- Commands to Configure Secure DHCP
- Commands to Configure DNS

Commands to Configure the System to be a DHCP Server

To configure the system to be a DHCP server, use the following commands.

**clear ip dhcp**

Reset the DHCP counters.

**Syntax**

```plaintext
clear ip dhcp [binding {address} | conflict | server statistics]
```

**Parameters**

- **binding**
  - Enter the keyword binding to delete all entries in the binding table.
- **address**
  - Enter the IP address to clear the binding entry for a single IP address.
- **conflicts**
  - Enter the keyword conflicts to delete all of the log entries created for IP address conflicts.
- **server statistics**
  - Enter the keywords server statistics to clear all the server counter information.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
debug ip dhcp server

Display Dell OS debugging messages for DHCP.

Syntax  
debug ip dhcp server [events | packets]

Parameters

- events  Enter the keyword events to display the DHCP state changes.
- packet   Enter the keyword packet to display packet transmission/reception.

Defaults

None

Command Modes

EXEC Privilege

Command History

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

Version                Description

9.8(1.0)                Introduced on the Z9100–ON.
9.8(0.0P5)              Introduced on the S4048-ON.
9.8(0.0P2)              Introduced on the S3048-ON.
9.7(0.0)                Introduced on the S6000-ON.
9.0.2.0                 Introduced on the S6000.
8.3.19.0                Introduced on the S4820T.
8.3.11.1                Introduced on the Z9000.
8.3.7.0                 Introduced on the S4810.
8.2.1.0                 Introduced on the C-Series and S-Series.

Usage Information

Press Enter after the clear ip dhcp binding command clears all the IPs from the binding table.
**debug ipv6 dhcp**

To enable debug logs for DHCPv6 relay agent transactions.

**Syntax**

default-router  

To disable the debug logs for dhcpv6 relay agent transactions, use the `debug ipv6 dhcp` command.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z-Series.</td>
</tr>
</tbody>
</table>

**default-router**

Assign a default gateway to clients based on the address pool.

**Syntax**

default-router address [address2...address8]

**Parameters**

- `address`  
  Enter a list of routers that may be the default gateway for clients on the subnet. You may specify up to eight routers. List them in order of preference.

**Defaults**

None

**Command Modes**

DHCP <POOL>

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
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
 CONFIGURATION
 DHCP <POOL>

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>
**dns-server**

Assign a DNS server to clients based on address pool.

Syntax

```plaintext
dns-server address [address2...address8]
```

Parameters

- **address**
  Enter a list of DNS servers that may service clients on the subnet. You may list up to eight servers, in order of preference.

Defaults

None

Command Modes

DHCP <POOL>

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**domain-name**

Assign a domain to clients based on the address pool.

Syntax

```plaintext
domain-name name
```

Parameters

- **name**
  Give a name to the group of addresses in a pool.

Defaults

None

Command Modes

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

### Version Description

- **9.8(1.0)**
  - Introduced on the Z9100-ON.
- **9.8(0.0P5)**
  - Introduced on the S4048-ON.
- **9.8(0.0P2)**
  - Introduced on the S3048-ON.
- **9.7(0.0)**
  - Introduced on the S6000-ON.
- **9.2(1.0)**
  - Introduced on the Z9500.
- **9.0.2.0**
  - Introduced on the S6000.
- **8.3.19.0**
  - Introduced on the S4820T.
- **8.3.11.1**
  - Introduced on the Z9000.
- **8.3.7.0**
  - Introduced on the S4810.
- **8.2.1.0**
  - Introduced on the C-Series and S-Series.

### excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

**Syntax**

excluded-address [address | low-address high-address]

**Parameters**

- **address**
  - Enter a single address to be excluded from the pool.
- **low-address**
  - Enter the lowest address in a range of addresses to be excluded from the pool.
- **high-address**
  - Enter the highest address in a range of addresses to be excluded from the pool.

**Defaults**

None

**Command Modes**

DHCP

**Command History**

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

**Version**

- **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.
hardware-address

For manual configurations, specify the client hardware address.

Syntax

```
hardware-address address
```

Parameters

- `address` Enter the hardware address of the client.

Defaults

None

Command Modes

DHCP <POOL>

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

Syntax

```
host address
```
lease

Specify a lease time for the addresses in a pool.

Syntax

```
lease {days [hours] [minutes] | infinite}
```

Parameters

- **days**: Enter the number of days of the lease. The range is from 0 to 31.
- **hours**: Enter the number of hours of the lease. The range is from 0 to 23.
- **minutes**: Enter the number of minutes of the lease. The range is from 0 to 59.
- **infinite**: Specify that the lease never expires.

Defaults

24 hours

Command Modes

DHCP <POOL>

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Dynamic Host Configuration Protocol (DHCP) | 493
netbios-name-server

Specify the NetBIOS Windows Internet Naming Service (WINS) name servers, in order of preference, that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

Syntax

netbios-name-server address [address2...address8]

Parameters

address

Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.

Defaults

None

Command Modes

DHCP <POOL>

Command History

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

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on the C-Series and S-Series.
netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as **hybrid**.

**Syntax**

```
netbios-node-type type
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Enter the NETBIOS node type:</td>
</tr>
</tbody>
</table>
|           | - Broadcast: Enter the keyword `b-node`.
|           | - Hybrid: Enter the keyword `h-node`.
|           | - Mixed: Enter the keyword `m-node`.
|           | - Peer-to-peer: Enter the keyword `p-node`.

**Defaults**

Hybrid

**Command Modes**

DHCP <POOL>

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

network

Specify the range of addresses in an address pool.

**Syntax**

```
network network /prefix-length
```
### Parameters

- **network/prefix-length**  
  Specify a range of addresses. Prefix-length range is from 17 to 31.

### Defaults

None

### Command Modes

DHCP `<POOL>`

### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

---

**pool**

Create an address pool.

### Syntax

```plaintext
pool name
```

### Parameters

- **name**  
  Enter the address pool's identifying name.

### Defaults

None

### Command Modes

DHCP

### Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
show ip dhcp binding

Display the DHCP binding table.

Syntax

show ip dhcp binding

Defaults

None

Command Modes

EXEC Privilege

Command History

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

Version Description

9.8(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.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on the C-Series and S-Series.

show ip dhcp configuration

Display the DHCP configuration.

Syntax

show ip dhcp configuration [global | pool name]

Parameters

pool name Display the configuration for a DHCP pool.
**show ip dhcp configuration global**

Display the DHCP configuration for the entire system.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip dhcp configuration global
Protocol status : Enabled
Number of ping packets : 1
Dell#
Dell# show ip dhcp configuration pool pl
Pool Name : pl
Pool Type : Dynamic
Domain Name : dell.com
Lease Time : 2Days 0Hrs 0Mins
DNS Servers : 10.11.0.1
Default Routers : 1.1.1.1
Network : 1.1.1.0 255.255.255.0
```

**show ip dhcp conflict**

Display the address conflict log.

**Syntax**

```
show ip dhcp conflict address
```

**Parameters**

- `address` : Display a particular conflict log entry.

**Defaults**

None

**Command Modes**

EXEC Privilege
**show ip dhcp server**

Display the DHCP server statistics.

**Syntax**

```
show ip dhcp server statistics
```

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>
Commands to Configure Secure DHCP

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

Syntax

```
arp inspection
```

Defaults

Disabled

Command Modes

INTERFACE VLAN

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `arp inspection-trust` — specify a port as trusted so that ARP frames are not validated against the binding table.

arp inspection-trust

Specify a port as trusted so that ARP frames are not validated against the binding table.

Syntax

```
arp inspection-trust
```

Defaults

Disabled
**Command Modes**
- INTERFACE
- INTERFACE PORT-CHANNEL

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `arp inspection` — enable dynamic ARP inspection on a VLAN.

---

**clear ip dhcp snooping**

Clear the DHCP binding table.

**Syntax**
clear ip dhcp snooping {binding | source-address-validation discard-counters [interface interface]}

**Parameters**
- `binding` Clears the binding table.
- `source-address-validation discard-counters` Clears discard counters from all the interfaces configured with IP Source Guard.
- `interface interface` (OPTIONAL) Specifies an interface to clear the discard counters.

Enter any of the following keywords and the interface information:
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.

**Defaults**
None

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Added the keywords discard-counters, interface, and the variable interface on the S4810, S4820T, S5000, S6000, Z9000, Z9500.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Example

The following example shows how to clear the discard counters globally:

Dell> clear ip dhcp snooping source-address-validation discard-counters

The following example shows how to clear the discard counters on an interface:

Dell> clear ip dhcp snooping source-address-validation discard-counters interface Gigabitethernet 1/10

The following example shows how to clear the discard counters on a port channel interface:

Dell> clear ip dhcp snooping source-address-validation discard-counters interface portchannel 1

Related Commands

- show ip dhcp snooping — display the contents of the DHCP binding table.

**clear ipv6 dhcp snooping binding**

Clear all the DHCPv6 snooping binding database entries.

**Syntax**

```
clear ipv6 dhcp snooping binding
```

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

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

Enable Option 82.

**Syntax**

```
ip dhcp relay information-option [remote-id | trust-downstream]
```

**Parameters**

- `remote-id`: Configure the system to enable the remote-id string in option-82.
- `trust-downstream`: Configure the system to trust Option 82 when it is received from the previous-hop router.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
</tbody>
</table>

### ip dhcp snooping

Enable DHCP snooping globally.

**Syntax**

```
[no] ip dhcp snooping
```

**Example**

```
Dell# clear ipv6 dhcp snooping?
binding    Clear the snooping binding database
```
Defaults
Disabled

Command Modes
CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the S4810 and S4820T.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the C-Series and S-Series on Layer 2 interfaces.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the C-Series and S-Series on Layer 3 interfaces.</td>
</tr>
</tbody>
</table>

Usage Information
When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table deletes and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Introduced in Dell Networking OS version 7.8.1.0, DHCP snooping was available for Layer 3 only and dependent on DHCP Relay Agent (ip helper-address). Dell Networking OS version 8.2.1.0 extends DHCP Snooping to Layer 2. You do not have to enable relay agent to snoop on Layer 2 interfaces.

**ipv6 dhcp snooping**

Enable DHCPv6 snooping globally for ipv6.

**Syntax**

```
[no] ipv6 dhcp snooping
```

To disable the snooping globally, use the no ipv6 dhcp snooping command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
</tbody>
</table>
**ipv6 dhcp snooping vlan**

Enable ipv6 DHCP Snooping on VLAN or range of VLANs.

**Syntax**

```
[no] ip dhcp snooping vlan <vlan-id>
```

To disable the ipv6 dhcp snooping on VLAN basis or range of VLAN, use the `no ipv6 dhcp snooping vlan <vlan-id>` command.

**Parameters**

- **vlan-id**
  
Enter the name of a VLAN id or list of the VLANs to enable DHCP Snooping.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
</tbody>
</table>

---

**ip dhcp snooping binding**

Create a static entry in the DHCP binding table.

**Syntax**

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface interface-type lease number
```

**Parameters**

- **mac address**
  
Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.

- **vlan-id**
  
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 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
lease time

Enter the keyword lease then the amount of time the IP address are leased. The range is from 1 to 4294967295.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- show ip dhcp snooping — display the contents of the DHCP binding table.

IPv6 DHCP Snooping Binding

Create a static DHCP snooping binding entry in the snooping database.

Syntax

[no] ipv6 dhcp snooping binding mac address vlan-id vlan-id ipv6 ipv6-address interface interface-type | interface-number lease value

Parameters

- **mac address**
  - Enter the keyword mac then the MAC address of the host to which the server is leasing the IPv6 address.

- **vlan-id**
  - Enter the keywords vlan-id then the VLAN to which the host belongs. The range is from 2 to 4094.

- **ipv6 ipv6-address**
  - Enter the keyword ipv6 then the IPv6 address that is leased to the client.

- **interface type**
  - Enter the keyword interface then the type of interface to which the host is connected:
For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.

For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

**interface number**
Enter the number of the interface.

**lease value**
Enter the keyword lease then the amount of time the IPv6 address are leased. The range is from 1 to 4294967295.

**Defaults**
None

**Command Modes**
- EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
</tbody>
</table>

### 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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.3.1.0 | Introduced on the E-Series.
7.8.1.0 | Introduced on the C-Series and S-Series.

**ipv6 dhcp snooping database write-delay**

To set time interval for storing the snooping binding entries in a file.

**Syntax**

```
[no] ipv6 dhcp snooping database write-delay value
```

To disable the storing of snooping binding entries in a file, use the `no ipv6 dhcp snooping write-delay` command.

**Parameters**

- **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

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.</td>
</tr>
</tbody>
</table>

**ip dhcp snooping database renew**

Renew the binding table.

**Syntax**

```
ip dhcp snooping database renew
```

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege
ipv6 dhcp snooping database renew

To load the binding entries from the file to DHCPv6 snooping binding database.

Syntax
ipv6 dhcp snooping database renew

Defaults
None

Command Modes
• EXEC Privilege

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

ip dhcp snooping trust

Configure an interface as trusted.

Syntax
[no] ip dhcp snooping trust

Dell Networking OS Command Line Reference Guide
Defaults
Command Modes
Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**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

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**ip dhcp source-address-validation**

Enable the IP Source Guard.

Syntax

```
[no] ip dhcp source-address-validation [ipmac] [vlan vlan-id]
```

Description

- Introduced on the Z9100-ON.
- Introduced on the S4048-ON.
- Introduced on the S3048-ON.
- Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmac</td>
<td>Enable IP+MAC Source Address Validation.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(OPTIONAL) SAV validates the source IP address along with the source VLAN ID against the DHCP snooping binding table.</td>
</tr>
</tbody>
</table>

Defaults

Disabled

Command Modes

INTERFACE

INTERFACE PORTCHANNEL

Command History

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Added the vlan keyword and the vlan-id variable. Introduced support for SAV on port channels interfaces.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added the keyword ipmac.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Allocate at least one FP block to ipmacacl before you can enable IP+MAC Source Address Validation and SAV with VLAN option.

1. Use the cam-acl 12acl command from CONFIGURATION mode.
2. Save the running-config to the startup-config.
3. Reload the system.

**ip dhcp relay information-option**

Enable Option 82.

**Syntax**

```
ip dhcp relay information-option [trust-downstream] [vpn]
```
trust-downstream

Configure the system to trust Option 82 when it is received from the previous-hop router.

vpn

Enter the keyword vpn to add VPN/VRF related sub-option to relay agent information Option 82.

**NOTE:** Adds the VPN/VRF related sub-options into the relay agent information option(82). When DHCP broadcasts are forwarded by the relay agent from clients to DHCP server.

**Default** Disabled.

**Command Modes** CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf)# ip dhcp relay information-option vpn
```

### ip dhcp snooping verify mac-address

Validate a DHCP packet’s source hardware address against the client hardware address field (CHADDR) in the payload.

**Syntax**

```
[no] ip dhcp snooping verify mac-address
```

**Defaults** Disabled

**Command Modes** CONFIGURATION

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
</tbody>
</table>
### ipv6 dhcp snooping verify mac-address

Configure to enable verify source mac-address against ipv6 DHCP packet mac address.

**Syntax**

```plaintext
[no] ipv6 dhcp snooping verify mac-address
```

To disable verify source mac-address against IPv6 DHCP packet MAC address, use the `no ipv6 dhcp snooping verify mac-address` command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

### ip helper-address

Configures the destination broadcast address or the host address for DHCP server requests.

**Syntax**

```
ip helper-address [vrf vrf-name] ip-address
```

To disable the destination broadcast address or the host address for DHCP server requests, use the `ip helper-address [vrf vrf-name] ip-address` command.
**Parameters**

- **vrf vrf-name** (Optional) Enter the keyword vrf and then the name of the VRF through which the host address can be reached.

- **ip-address** Enter an IP address through which the host address can be reached.

**Default**

Disabled.

**Command Modes**

INTERFACE

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>Version 9.4.(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command on the interfaces where the DHCP clients are connected to forward the packets from clients to DHCP server and vice-versa.

**Example**

```
Dell(conf-if-gi-1/12)# ip helper-address vrf jay 10.0.0.2
```

### ipv6 helper-address

Configures the ipv6 DHCP helper addresses without VRF.

**Syntax**

```
[no] ipv6 helper-address ipv6-address
```

To delete the ipv6 helper address, use the [no] ipv6 helper-address ipv6-address command.

**Parameters**

- **ipv6-address** Enter the keyword ipv6-address through which the server address can be reached.

**Default**

Disabled.

**Command Modes**

INTERFACE

**Command History**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, S6000-ON, Z9000, and Z9500.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command on the interfaces where the DHCP clients are connected to forward the packets from clients to DHCP server and vice-versa.
Example

Dell(conf-if-gi-1/1)# ipv6 helper-address
X::X:X::X     IPv6 helper address
VRF            VRF name.
Global         Global address space

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

Syntax

show ip dhcp snooping [binding | source-address-validation [discard-counters [interface interface]]]

Parameters

Parameters | Description
---|---
binding | Display the binding table.
source-address-validation | Display the interfaces configured with IP Source Guard.
discard-counters | (OPTIONAL) Display the number of dropped packets.
interface interface | (OPTIONAL) Specifies an interface to show the discard counters.

Enter any of the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

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

Version | Description
---|---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.6(0.0) | Added the discard-counters, interface keywords, and the interface variable.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
Example

The following example displays the interfaces configured with IP Source Guard:

```
Dell> show ip dhcp snooping source-address-validation
ip sav access-list on GigabitEthernet 1/1
Total cam count 3
permit host 0.0.0.0 count (0 packets)
permit host 10.1.1.252 count (0 packets)
permit host 10.1.1.253 count (0 packets)
ipmac-vlan sav access-list on GigabitEthernet 1/2
Total cam count 4
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 10.1.1.1 host 00:00:00:aa:00:01 count (0 packets)
permit vlan 10 host 10.1.1.2 host 00:00:00:aa:00:02 count (0 packets)
permit vlan 20 host 10.2.2.1 host 00:00:00:aa:00:03 count (0 packets)
permit vlan 20 host 10.2.2.2 host 00:00:00:aa:00:04 count (0 packets)
```

```
The following example displays the port channel interfaces configured with IP Source Guard:

Dell> show ip dhcp snooping source-address-validation interface portchannel 10
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 1
Total cam count 5
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 2
Total cam count 5
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 3
Total cam count 5
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)
```

```
NOTE: The output for port-channel interfaces does not display the physical interface.
```

The following example displays the SAV discard counters on all interfaces:

```
Dell> show ip dhcp snooping source-address-validation discard-counters
deny access-list on GigabitEthernet 1/1
Total cam count 1
deny count (0 packets)
deny access-list on GigabitEthernet 1/2
Total cam count 2
deny vlan 10 count (0 packets)
deny vlan 20 count (0 packets)
```

The following example displays the SAV discard counters on a particular interface:

```
Dell> show ip dhcp snooping source-address-validation discard-counters
interface GigabitEthernet 1/1
deny access-list on GigabitEthernet 1/1
Total cam count 2
```
deny vlan 10 count (0 packets)
deny vlan 20 count (0 packets)

The following example displays the SAV discard counters on a port channel interface:

Dell> show ip dhcp snooping source-address-validation discard-counters
interface portchannel 10
deny access-list on Port-channel 10 on stack-unit 1
Total cam count 1
deny vlan 10 count (0 packets)
deny access-list on Port-channel 10 on stack-unit 2
Total cam count 1
deny vlan 10 count (0 packets)
deny access-list on Port-channel 10 on stack-unit 3
Total cam count 1
deny vlan 10 count (0 packets)

NOTE: The output for port-channel interfaces does not display the physical interface. If the LAG member interfaces belong to different stack-units, the counters are displayed per stack-unit for that port channel.

show ipv6 dhcp snooping

Display the DHCPv6 snooping binding database.

Syntax
show ipv6 dhcp snooping

Defaults
None

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S4810, S4820T, S6000, S6000-ON, and Z-Series.

Example
Dell# show ipv6 dhcp snooping
IPv6 DHCP Snooping : Enabled.
IPv6 DHCP Snooping Mac Verification : Disabled.

Database write-delay (In minutes) : 5

DHCP packets information
Snooping packets : 0
Snooping packets processed on L2 vlans : 0

DHCP Binding File Details
Invalid File : 0
Invalid Binding Entry : 0
Binding Entry lease expired : 0

Dell#
Commands to Configure DNS

To configure the Domain Names Systems (DNS) on the system, use the following commands:

**ip name-server**

Configures one or more name server (DNS) IP addresses. You can configure up to six IP addresses.

**Syntax**

```
ip name-server [vrf vrf-name] ip-address [ip-address2] [ip-address3] [ip-address4] [ip-address5] [ip-address6]
```

To undo the name server ip address configuration for VRF, use the `no ip name-server [vrf vrf-name] ip-address` command.

**Parameters**

- **vrf vrf-name**
  - (Optional) Enter the key word `vrf` and then the name of the VRF to configure the name server IP addresses for that VRF.
- **ip-address [ip-address2] [ip-address3] [ip-address4] [ip-address5] [ip-address6]**
  - Enter the IP address of the name server in dotted decimal format.

**NOTE:** Use the additional `ip-address` parameters (ip-address2 to ip-address6) in a sequential order to specify up to a maximum of six IP addresses per VRF.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to associate the system with one or more DNS servers.

In a dual stack setup, the system sends both A (request for IPv4 — RFC 1035) and AAAA (request for IPv6 — RFC 3596) record requests to a DNS server even if only the `ip name-server` command is configured.

**Example**

```
• Dell(conf)#ip name-server vrf jay 2.2.2.2
• Dell(conf)#ip name-server vrf jay 2.2.2.2 3.3.3.3 4.4.4.4 5.5.5.5 6.6.6.6 7.7.7.7
```
**ip domain-name**

Configures the default domain corresponding to a specific VRF. This domain is appended to the incomplete DNS requests corresponding to the specified VRF.

**Syntax**

```plaintext
ip domain-name [vrf vrf-name] name
```

To undo the domain name configuration corresponding to a specific VRF, use the `no ip domain-name [vrf vrf-name] name` command.

**Parameters**

- **vrf vrf-name** (Optional) Enter the key word `vrf` and then the name of the VRF to configure the domain corresponding to that VRF.
- **name** Enter the name of the domain to be appended to the incomplete DNS requests corresponding to the specified VRF.

**Defaults**

None

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to configure a domain name corresponding to a VRF. This domain is appended to the incomplete DNS requests corresponding to the specified VRF.

**Example**

```
Dell(conf)# ip domain-name vrf jay dell.com
```

**ip domain-list**

Adds a domain name to the DNS list. This domain name is appended to incomplete host names in DNS requests corresponding to a specific VRF.

**Syntax**

```plaintext
ip domain-list [vrf vrf-name] name
```

To remove a domain name from DNS list, use the `no ip domain-list [vrf vrf-name] name` command.
**Parameters**

- **vrf vrf-name**
  - (Optional) Enter the key word `vrf` and then the name of the VRF to add a domain name to the DNS list corresponding to that VRF.
- **name**
  - Enter the name of the domain to be appended to the DNS list corresponding to the VRF.

**Defaults**

None

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to add domain names to the DNS lists corresponding to a specific VRF. You can add up to a maximum of six domain names to the DNS list corresponding to a VRF. This domain is used to complete the unqualified host names.

**Example**

```plaintext
Dell(conf)# ip domain-list vrf jay dell.com
Dell(conf)# ip domain-list vrf jay force10.com
```

**ip host**

Configures a mapping between the host name server and the IP address for a specific VRF. This mapping information is used by the name-to-IP address table to resolve host names.

**Syntax**

```plaintext
ip host [vrf vrf-name] name ip-address
```

To undo the host name server to IP address mapping for VRFs, use the `no ip host [vrf vrf-name] name ip-address` command.

**Parameters**

- **vrf vrf-name**
  - (Optional) Enter the key word `vrf` and then the name of the VRF to configure the name server to IP address mapping for that VRF.
- **name**
  - Enter the name of the host to be associated with an IP address.
- **ip-address**
  - Enter the IP address of the name server in dotted decimal format.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Usage Information
Use this command to create a mapping between a host name server and its IP addresses for a specific VRF.

Example
Dell(conf)# ip host vrf jay dell 1.1.1.1

clear host

Removes one or all dynamically learned host table entries for a specific VRF.

Syntax
clear host [vrf vrf-name] {* | host-name}

Parameters
vrf vrf-name
(Optional) Enter the key word vrf and then the name of the VRF to delete dynamically learned host table entries corresponding to that VRF.

host-name
Enter the name of the host corresponding to which you want to delete the dynamically learnt host table entries.

* Enter * to delete all host table entries.

Defaults
None

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.4.(0.0) Introduced on the S-Series and Z-Series.

Usage Information
Use this command to delete one or all dynamically learned host table entries corresponding to a specific VRF.

Example
Dell# clear host vrf jay dell
Dell# clear host vrf jay *

Dynamic Host Configuration Protocol (DHCP)
Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) supports multiple "best paths" in next-hop packet forwarding to a destination device.

Topics:
- `ecmp-group`
- `hash-algorithm`
- `hash-algorithm ecmp`
- `hash-algorithm seed`
- `ip ecmp-group`
- `ip ecmp weighted`
- `link-bundle-monitor enable`
- `link-bundle-distribution trigger-threshold`
- `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.

**Syntax**

```
ecmp-group {ecmp-group-id interface interface | link-bundle-monitor}
```

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

**Parameters**

- **ecmp-group ID**
  Enter the identifier number for the ECMP group. The range is from 2 to 64.

- **interface**
  Enter the following keywords and the interface information to add the interface to the ECMP group:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a LAG interface, enter the keywords `port-channel` then the slot/port information.

**Defaults**

Off
hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a Port Channel and ECMP. The ECMP and LAG options are supported on the S-Series and Z-Series.

Syntax

```
hash-algorithm {algorithm-number | (ecmp {crc16 | crc16cc | crc32MSB | crc32LSB | crc-upper | dest-ip | lsb | xor1 | xor2 | xor4 | xor8 | xor16} [number] hg | stack-unit stack-unit-number | port-set port-pipe | hg-seed seed-value stack-unit | lag {checksum | crc | xor} [number] nh-ecmp {checksum | crc | xor} [number] stack-unit number ip-sa-mask value | ip-da-mask value | seed seed-value } }
```

To return to the default hash algorithm, use the no hash-algorithm command.

To return to the default ECMP hash algorithm, use the no hash-algorithm ecmp algorithm-value command.

Parameters

- `ecmp crc16 | crc16cc | crc32MSB | crc32LSB | crc-upper | dest-ip | lsb`: Enter the keyword `ecmp` then one of the following options:
  - `crc16`: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)
  - `crc16cc`: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial
  - `crc32MSB`: Use CRC32_UPPER — MSB 16 bits of computed CRC32
  - `crc32LSB`: Use CRC32_LOWER — LSB 16 bits of computed CRC32
  - `crc-upper`: Uses the upper 32 bits of the key for the hash computation
Equal Cost Multi-Path (ECMP)

- `dest-ip`: Uses the destination IP for ECMP hashing
- `lsb`: Returns the LSB of the key as the hash
- `xor1`: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- `xor2`: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- `xor4`: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- `xor8`: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- `xor16`: Use CR16 — 16 bit XOR

**hg**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crc16</code></td>
<td>Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default)</td>
</tr>
<tr>
<td><code>crc16cc</code></td>
<td>Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial</td>
</tr>
<tr>
<td><code>crc32MSB</code></td>
<td>Use CRC32_UPPER — MSB 16 bits of computed CRC32</td>
</tr>
<tr>
<td><code>crc32LSB</code></td>
<td>Use CRC32_LOWER — LSB 16 bits of computed CRC32</td>
</tr>
<tr>
<td><code>xor1</code></td>
<td>Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1</td>
</tr>
<tr>
<td><code>xor2</code></td>
<td>Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2</td>
</tr>
<tr>
<td><code>xor4</code></td>
<td>Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4</td>
</tr>
<tr>
<td><code>xor8</code></td>
<td>Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8</td>
</tr>
<tr>
<td><code>xor16</code></td>
<td>Use CR16 — 16 bit XOR</td>
</tr>
</tbody>
</table>

Enter the keyword `hg` then one of the following options:

- `stack-unit-number`: Enter the stack-unit number.
- `port-set port-pipe`: Enter the port-pipe number. The range is from 0 to 5.

**hg-seed**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seed-value</code></td>
<td>Enter the hash algorithm seed value. The range is from 0 to 2147483646.</td>
</tr>
</tbody>
</table>

Enter the keywords `hg-seed` then the stack unit number, then the stack-unit port-pipe number.

**lag**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hash algorithm</code></td>
<td>Enter the hash algorithm seed value. The range is from 0 to 47.</td>
</tr>
</tbody>
</table>

**nh-ecmp**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hashalgorithm</code></td>
<td>(OPTIONAL) Enter the keyword <code>nh-ecmp</code> then the ECMP hash algorithm value.</td>
</tr>
<tr>
<td><code>value</code></td>
<td>(OPTIONAL) : Enter the keyword <code>stack-unit</code> then the stack-unit slot number.</td>
</tr>
</tbody>
</table>

**ip-sa-mask**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>(OPTIONAL) Enter the keyword <code>ip-sa-mask</code> then the ECMP/LAG hash mask value. The range is from 0 to FF.</td>
</tr>
</tbody>
</table>

**ip-da-mask**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>(OPTIONAL) Enter the keyword <code>ip-da-mask</code> then the ECMP/LAG hash mask value. The range is from 0 to FF.</td>
</tr>
</tbody>
</table>
Defaults

IPSA and IPDA mask value is **FF** for the stack-unit.

Command Modes

**CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Added flow-based-hashing support for hashing on ECMP for S4820T, S6000, S4048 and Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added the <strong>nh-ecmp</strong> option.</td>
</tr>
<tr>
<td>7.7.1.1</td>
<td>Added the <strong>nh-ecmp</strong> option.</td>
</tr>
</tbody>
</table>

Usage Information

To ensure that CRC is not used for LAG, set the default hash-algorithm method on E-Series systems. For example:

```
hash-algorithm ecmp xor lag checksum nh-ecmp checksum.
```

The hash value calculated with the `hash-algorithm` command is unique to the entire unit. The hash algorithm command with the stack-unit option changes the hash for a particular stack-unit by applying the mask specified in the IPSA and IPDA fields.

The stack-unit option is applicable with the lag-hash-align microcode only. Any other microcode returns an error message as follows:

```
Dell(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff
% Error: This command is not supported in the current microcode configuration
```

In addition, the linecard number **ip-sa-mask** value **ip-da-mask** value option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the **ip-sa-mask** and **ip-da-mask** values must be equal. (Single Linecard).
- When hashing is done only on IPSA or IPDA, Dell Networking OS maintains bi-directionality with masks set to **XX 00** for stack-unit 1 and **00 XX** for stack-unit 2 (**ip-sa-mask** and **ip-da-mask**). The mask value must be the same for both stack-units when using multiple stack-units as ingress (where **XX** is any value from 00 to FF for both stack-units). For example, assume that traffic is flowing between linecard 1 and linecard 2:

```
hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00
hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa
```

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm

---

**Equal Cost Multi-Path (ECMP)**

525
does not provide a satisfactory distribution of traffic, use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculted to balance traffic across the members.

**hash-algorithm ecmp**

Change the hash algorithm used to distribute traffic flows across an ECMP (equal-cost multipath routing) group.

<table>
<thead>
<tr>
<th>Term heading</th>
<th>Description heading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>hash-algorithm ecmp {crc-upper}</td>
</tr>
<tr>
<td></td>
<td>To return to the default hash algorithm, use the no hash-algorithm ecmp command.</td>
</tr>
<tr>
<td>Parameters</td>
<td>crc-upper: Uses the upper 32 bits of the key for the hash computation. The default is crc-lower.</td>
</tr>
<tr>
<td></td>
<td>dest-ip: Uses the destination IP for ECMP hashing. The default is enabled.</td>
</tr>
<tr>
<td></td>
<td>lsb: Returns the LSB of the key as the hash. The default is crc-lower.</td>
</tr>
<tr>
<td>Defaults</td>
<td>• crc-lower</td>
</tr>
<tr>
<td></td>
<td>• dest-ip enabled</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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.
Term heading | Description heading
---|---
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.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>hash-algorithm seed value [stack-unit slot/port] [port-set number]</th>
</tr>
</thead>
</table>

**Parameters**

- **seed value**: Enter the keyword `seed` then the seed value. The range is from 0 to 2,147,483,646.
- **stack-unit slot/port**: Enter the keyword `stack-unit` then the slot/port number.
- **port-set number**: Enter the keyword `port-set` then the port-pipe number. The value is 0.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.

Dell 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 {number}` command.

**Parameters**

- `maximum-paths`: Specify the maximum number of ECMP for a route. The range is 2 to 64.
- `path-fallback`: Use the keywords `path-fallback` to enable this feature. If you enable the feature, re-enter this keyword to disable the feature.

**Defaults**

- 16

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**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.
**ip ecmp weighted**

Enables weighted ECMP calculations.

**Syntax**

```
ip ecmp weighted
```

To disable weighted ECMP calculations, enter the `no ip ecmp weighted` command.

**Defaults**

N/A

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Enabling this CLI would inform the FIB to re-program the destination prefix paths with weights in the HW/CAM on the fly.

If disabled, the CLI would inform the FIB to re-program the destination prefix paths with no weights or regular ECMP.

**Example**

```
Dell(conf)# ip ecmp ?
weight* weighted Enables Weighted ECMP
Dell(conf)# ip ecmp weighted
Dell(conf)# do show running-config | grep ecmp
  ip ecmp weighted
Dell(conf)#
Dell(conf)# no ip ecmp ?
weight* weighted Enables Weighted ECMP
Dell(conf)# no ip ecmp weighted
Dell(conf)# do show running-config | grep ecmp
```

**link-bundle-monitor enable**

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

**Syntax**

```
link-bundle-monitor enable
```

To exit from ECMP group mode, use the `exit` command.

**Command Modes**

- ECMP-GROUP
- PORT-CHANNEL INTERFACE
**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**link-bundle-distribution trigger-threshold**

Provides a mechanism to set the threshold to trigger when traffic distribution begins being monitored on an ECMP link bundle.

**Syntax**

```
link-bundle-distribution trigger-threshold [percent]
```

To exit from ecmp group mode, use the `exit` command.

**Parameters**

- `percent` Indicate the threshold value when traffic distribution starts being monitored on an ECMP link bundle. The range is from 1 to 90%. The default is 60%.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### show config

Display the ECMP configuration.

**Syntax**

```
show config
```  

**Command Modes**

CONFIGURATION-ECMP-GROUP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show running-config ecmp-group` — display interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution.

### show link-bundle distribution

Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

**Syntax**

```
show link-bundle-distribution
```  

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Dell# show link-bundle-distribution
Link-bundle trigger threshold - 30

<table>
<thead>
<tr>
<th>ECMP bundle</th>
<th>Utilization [In Percent]</th>
<th>Alarm State</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>0</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Line Protocol</th>
<th>Utilization [In Percent]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 1/1</td>
<td>Up</td>
<td>0</td>
</tr>
<tr>
<td>Po 128</td>
<td>Up</td>
<td>0</td>
</tr>
<tr>
<td>Po 100</td>
<td>Up</td>
<td>0</td>
</tr>
</tbody>
</table>

Dell#
To configure federal information processing standards (FIPS) cryptography, use the following commands:

**Topics:**
- `fips mode enable`
- `show fips status`
- `show ip ssh`
- `ssh`

### fips mode enable

Enable the FIPS cryptography mode on the platform.

**Syntax**

```
[no] fips mode enable
```

To disable the FIPS cryptography mode, use the `no fips mode enable` command.

**Default**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**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)#
```

### show fips status

Displays the status of the FIPS mode.

**Syntax**

```
show fips status
```
show ip ssh

Display information about established SSH sessions.

Syntax

show ip ssh

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Removed the support for hmac-sha2-256-96 algorithm.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Example
Dell# show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
SSH server vrf            : default.
SSH server ciphers        : aes256-ctr, aes256-cbc, aes192-ctr, aes192-cbc,
aes128-ctr, aes128-cbc, 3des-cbc.
SSH server macs           : hmac-sha2-256, hmac-shal, hmac-shal-96, hmac-md5, hmac-md5-96.
SSH server kex algorithms : diffie-hellman-group-exchange-sha1,diffie-hellman-
group1-shal,diffie-hellman-group14-shal.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA Authentication       : disabled.
Vty          Encryption      HMAC            Remote IP
  2            aes128-cbc      hmac-md5        10.16.127.141
  4            aes128-cbc      hmac-md5        10.16.127.141
  * 5           aes128-cbc      hmac-md5        10.16.127.141
Dell#

Related Commands
• ip ssh server — configures an SSH server.
• show ip ssh client-pub-keys — displays the client-public keys.

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 alogorithm|-p port-number|-v {1|2}]

Parameters
hostname  (OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address  (OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6 addressprefix  (OPTIONAL) Enter the IPv6 address in the x:x:x:x format then the prefix length in the /x format. The range is from /0 to /128

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

-c encryption cipher  Enter the following encryption cipher to use. (For v2 clients only.)
  • 3des-cbc: Force ssh to use 3des-cbc encryption cipher.

  FIPS mode is enabled or disabled:
  • aes256-ctr: Force ssh to use the aes256-ctr encryption cipher.
  • aes256-cbc: Force ssh to use the aes128-cbc encryption cipher.
  • aes192-ctr: Force ssh to use the aes128-cbc encryption cipher.
  • aes192-cbc: Force ssh to use the aes256-cbc encryption cipher.
  • aes128-ctr: 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-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm.
  - hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm.
  - hmac-md5-96: Force ssh to use the hmac-md5-96 HMAC algorithm.
  - hmac-md5: Force ssh to use the hmac-md5 HMAC algorithm.

With the FIPS mode enabled:
  - hmac-sha2-256: Force ssh to use the hmac-sha2-256 HMAC algorithm.
  - hmac-sha1-96: Force ssh to use the hmac-sha1-96 HMAC algorithm.
  - hmac-sha1: Force ssh to use the hmac-sha1 HMAC algorithm.
  - hmac-md5-96: Force ssh to use the hmac-md5-96 HMAC algorithm.
  - hmac-md5: Force ssh to use the hmac-md5 HMAC algorithm.

-p port-number  (OPTIONAL) Enter the keyword -p then the port number.
The range is 1 to 65535.

-v {1|2}  (OPTIONAL) Enter the keyword -v then the SSH version 1 or 2.
The default: The version from the protocol negotiation.

SEE NOTE: If the FIPS mode is enabled, this option does not display in the output.

Defaults
See Parameters.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Removed the support for hmac-sha2-256-96 algorithm.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Related Commands
ip ssh server  Configure an SSH server.
show ip ssh client-pub-keys  Display the client-public keys.
Usage Information

Dell Networking OS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

Example

If FIPS mode is not enabled:

Dell# ssh 10.10.10.10 ?
-c Encryption cipher to use (for v2 clients only)
-l User name option
-m HMAC algorithm to use (for v2 clients only)
-p SSH server port option (default 22)
-v SSH protocol version

Dell# ssh 10.10.10.10 -c ?
3des-cbc Force ssh to use 3des-cbc encryption cipher
aes128-cbc Force ssh to use aes128-cbc encryption cipher
aes192-cbc Force ssh to use aes192-cbc encryption cipher
aes256-cbc Force ssh to use aes256-cbc encryption cipher
aes128-ctr Force ssh to use aes128-ctr encryption cipher
aes192-ctr Force ssh to use aes192-ctr encryption cipher
aes256-ctr Force ssh to use aes256-ctr encryption cipher

Dell# ssh 10.10.10.10 -m ?
hmac-md5 Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96 Force ssh to use hmac-md5-96 HMAC algorithm
hmac-sha1 Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-sha2-256 Force ssh to use hmac-sha2-256 HMAC algorithm

With FIPS mode enabled:

Dell# ssh 10.10.10.10 ?
-c Encryption cipher to use (for v2 clients only)
-l User name option
-m HMAC algorithm to use (for v2 clients only)
-p SSH server port option (default 22)

Dell# ssh 10.10.10.10 -c ?
3des-cbc Force ssh to use 3des-cbc encryption cipher
aes128-cbc Force ssh to use aes128-cbc encryption cipher
aes192-cbc Force ssh to use aes192-cbc encryption cipher
aes256-cbc Force ssh to use aes256-cbc encryption cipher
aes128-ctr Force ssh to use aes128-ctr encryption cipher
aes192-ctr Force ssh to use aes192-ctr encryption cipher
aes256-ctr Force ssh to use aes256-ctr encryption cipher

Dell# ssh 10.10.10.10 -m ?
hmac-sha1 Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-sha2-256 Force ssh to use hmac-sha2-256 HMAC algorithm

FIPS Cryptography | 537
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 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.

**Syntax**

```
clear frrp [ring-id]
```

**Parameters**

- **ring-id**

  (Optional) Enter the ring identification number. The range is from 1 to 255.

**Defaults**

None

**Command Modes**

EXEC
Clear FRRP statistics counters.

**Syntax**
```
debug frrp {event | packet | detail} [ring-id] [count number]
```

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**
Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. Dell Networking OS requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

**Example**
```
Dell# clear frrp
Clear frrp statistics counter on all ring [confirm] yes
Dell# clear frrp 4
Clear frrp statistics counter for ring 4 [confirm] yes
Dell#
```

**Related Commands**
- `show frrp` — display the Resilient Ring Protocol configuration.
To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [count-number]` command.

**Parameters**

- **event**
  - Enter the keyword `event` to display debug information related to ring protocol transitions.

- **packet**
  - Enter the keyword `packet` to display brief debug information related to control packets.

- **detail**
  - Enter the keyword `detail` to display detailed debug information related to the entire ring protocol packets.

- **ring-id**
  - (Optional) Enter the ring identification number. The range is from 1 to 255.

- **count number**
  - Enter the keyword `count` then the number of debug outputs. The range is from 1 to 65534.

**Defaults**

- Disabled.

**Command Modes**

- `CONFIGURATION (conf-frrp)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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**

**Word**
Enter a description of the ring. Maximum: 255 characters.

**Defaults**
None

**Command Modes**
CONFIGURATION (conf-frrp)

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**disable**

Disable the resilient ring protocol.

**Syntax**
disable

To enable the Resilient Ring Protocol, use the no disable command.

**Defaults**
Disabled

**Command Modes**
CONFIGURATION (conf-frrp)

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
interface

Configure the primary, secondary, and control-vlan interfaces.

Syntax

interface {primary interface secondary interface control-vlan vlan-id}
To return to the default, use the no interface {primary interface secondary interface control-vlan vlan-id} command.

Parameters

- **primary interface**
  - Enter the keyword primary to configure the primary interface then one of the following interfaces and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a port channel interface, enter the keywords port-channel then a number.

- **secondary interface**
  - Enter the keyword secondary to configure the secondary interface then one of the following interfaces and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a port channel interface, enter the keywords port-channel then a number.

- **control-vlan vlan-id**
  - Enter the keyword control-vlan then the VLAN ID. The range is from 1 to 4094.

Defaults

None

Command Modes

CONFIGURATION (conf-frrp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**Version**  | **Description**  
---|---
9.10(0.0) | Introduced on the S6100-ON. 
9.8(1.0) | Introduced on the Z9100-ON. 
9.8(0.0P5) | Introduced on the S4048-ON. 
9.8(0.0P2) | Introduced on the S3048-ON. 
9.7(0.0) | Introduced on the S6000-ON. 
9.2(1.0) | Introduced on the Z9500. 
9.0.2.0 | Introduced on the S6000. 
8.3.19.0 | Introduced on the S4820T. 
8.3.11.1 | Introduced on the Z9000. 
8.3.7.0 | Introduced on the S4810. 
8.2.1.0 | Introduced on the C-Series. 
7.4.1.0 | Introduced. 

**Usage Information**
This command causes the Ring Manager to take ownership of the two ports after IFM validates the configuration. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

**Related Commands**
- `show frrp` — display 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-frrp)

**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. 
9.8(1.0) | Introduced on the Z9100-ON. 
9.8(0.0P5) | Introduced on the S4048-ON. 

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-frrp)

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.

9.8(1.0)Introduced on the Z9100-ON.

9.8(0.0P5)Introduced on the S4048-ON.

9.8(0.0P2)Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

8.2.1.0 Introduced on the C-Series.

7.4.1.0 Introduced.
**protocol frrp**

Enter the Resilient Ring Protocol and designate a ring identification.

**Syntax**

```
protocol frrp {ring-id}
```

To exit the ring protocol, use the no `protocol frrp {ring-id}` command.

**Parameters**

- `ring-id`: Enter the ring identification number. The range is from 1 to 255.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**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

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.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on the C-Series.
7.4.1.0 Introduced.
```

Usage Information

Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. Dell Networking OS requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

```
Usage Information

Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. Dell Networking OS requires a command line confirmation before the command is executed. This command clears the following counters:

- hello Rx and Tx counters
```
• Topology change Rx and Tx counters
• The number of state change counters

Example (Summary)

Dell# show frrp summary

<table>
<thead>
<tr>
<th>Ring-ID</th>
<th>State</th>
<th>Mode</th>
<th>Ctrl_Vlan</th>
<th>Member_Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>UP</td>
<td>Master</td>
<td>2</td>
<td>11-20, 25, 27-30</td>
</tr>
<tr>
<td>31</td>
<td>UP</td>
<td>Transit</td>
<td>31</td>
<td>40-41</td>
</tr>
<tr>
<td>50</td>
<td>Down</td>
<td>Transit</td>
<td>50</td>
<td>32</td>
</tr>
</tbody>
</table>

Dell#

Example (1)

Dell# show frrp 1

Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary: GigabitEthernet 1/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009

Dell#

Example (2)

Dell# show frrp 2 summary

Dell# show frrp 2 summary

<table>
<thead>
<tr>
<th>Ring-ID</th>
<th>State</th>
<th>Mode</th>
<th>Ctrl_Vlan</th>
<th>Member_Vlans</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Up</td>
<td>Master</td>
<td>2</td>
<td>11-20, 25, 27-30</td>
</tr>
</tbody>
</table>

Dell#

Related Commands

- protocol frrp — enter 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)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

The `hello interval` command is the interval at which ring frames are generated from the primary interface of the master node. The `dead interval` command is the time that elapses before a time-out occurs.
GARP VLAN Registration (GVRP)

The Dell Networking operating system supports the basic GVRP commands on the Dell Networking OS.

The generic attribute registration protocol (GARP) mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

• The GVRP application
• GARP information propagation (GIP)
• GARP information declaration (GID)

Important Points to Remember

• GVRP is supported on Layer 2 ports only.
• All VLAN ports added by GVRP are tagged.
• GVRP is supported on untagged ports belonging to a default VLAN and tagged ports.
• GVRP cannot be enabled on untagged ports belonging to a non-default VLAN unless native VLAN is turned on.
• GVRP requires end stations with dynamic access NICs.
• Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
• On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
• GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
• GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
• GVRP operates only on ports that are in the STP forwarding state. If you enable GVRP, a port that changes to the STP Forwarding state automatically begin to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
• VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
• GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge must classify and analyze packets by VLAN protocols, manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge must know only how to reach a given VLAN, then GVRP provides all necessary information.
• The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

Topics:
clear gvrp statistics

Clear GVRP statistics on an interface.

Syntax

```
clear gvrp statistics interface interface
```

Parameters

- `interface interface` Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.

Defaults

None

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
**debug gvrp**

Enable debugging on GVRP.

**Syntax**

```
debug gvrp {config | events | pdu}
```

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

**Parameters**

- **config**
  - Enter the keyword `config` to enable debugging on the GVRP configuration.
- **event**
  - Enter the keyword `event` to enable debugging on the JOIN/LEAVE events.
- **pdu**
  - Enter the keyword `pdu` then one of the following Interface keywords and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a port channel interface, enter the keywords `port-channel` then a number.

**Defaults**

Disabled.

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
disable

Globally disable GVRP.

Syntax
disable

To re-enable GVRP, use the no disable command.

Defaults
Enabled.

Command Modes
CONFIGURATION-GVRP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on C-Series, E-Series, and S-Series

Related Commands
- gvrp enable — enable GVRP on physical interfaces and LAGs.
- protocol gvrp — access GVRP protocol.
garp timers

Set the intervals (in milliseconds) for sending GARP messages.

Syntax

garp timers {join | leave | leave-all}

To return to the previous setting, use the no garp timers {join | leave | leave-all} command.

Parameters

- **join**: Enter the keyword `join` then the number of milliseconds to configure the join time. The range is from 100 to 147483647 milliseconds. The default is **200 milliseconds**.

  | NOTE: Designate the milliseconds in multiples of 100.

- **leave**: Enter the keyword `leave` then the number of milliseconds to configure the leave time. The range is from 100 to 2147483647 milliseconds. The default is **600 milliseconds**.

  | NOTE: Designate the milliseconds in multiples of 100.

- **leave-all**: Enter the keywords `leave-all` then the number of milliseconds to configure the leave-all time. The range is from 100 to 2147483647 milliseconds. The default is 1000 milliseconds.

  | NOTE: Designate the milliseconds in multiples of 100.

Defaults

As above.

Command Modes

CONFIGURATION-GVRP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>
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 re-registration 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` — display the current GARP times.

**gvrp enable**

Enable GVRP on physical interfaces and LAGs.

Syntax

```
gvrp enable
```

To disable GVRP on the interface, use the `no gvrp enable` command.

Defaults

Disabled.

Command Modes

- CONFIGURATION-INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

Related Commands

- `disable` — globally disable GVRP.
gvrp registration

Configure the GVRP register type.

Syntax

gvrp registration {fixed | normal | forbidden}
To return to the default, use the gvrp register normal command.

Parameters

fixed
Enter the keyword fixed then the VLAN range in a comma-separated VLAN ID set.

normal
Enter the keyword normal then the VLAN range in a comma-separated VLAN ID set.
This setting is the default.

forbidden
Enter the keyword forbidden then the VLAN range in a comma-separated VLAN ID set.

Defaults

normal

Command Modes

CONFIGURATION-INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on C-Series, E-Series, and S-Series

Usage Information

Fixed registration prevents an interface, configured using the command line, to belong to a VLAN (static configuration) from being unconfigured when it receives a Leave message. Therefore, Registration mode on that interface is fixed.

Normal registration is the default registration. The port’s membership in the VLAN depends on GVRP. The interface becomes a member of a VLAN after learning about the VLAN through GVRP. If the VLAN is removed from the port that sends GVRP advertisements to this device, the port stops being a member of the VLAN.
To advertise or learn about VLANs through GVRP, use the `forbidden` command when you do not want the interface.

**Related Commands**
- `show gvrp` — display the GVRP configuration including the registration.

### protocol gvrp

**Access GVRP protocol — (config-gvrp)#.**

**Syntax**

```
protocol gvrp
```

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**Related Commands**
- `disable` — globally disable GVRP.

### show config

Display the global GVRP configuration.

**Syntax**

```
show config
```
**show garp timers**

Display the GARP timer settings for sending GARP messages.

**Syntax**

```
show garp timers
```

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**Related Commands**

- `gvrp enable` — enable GVRP on physical interfaces and LAGs.
- `protocol gvrp` — access the GVRP protocol.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show garp timers
GARP Timers      Value (milliseconds)
----------------------------------------
Join Timer        200
Leave Timer       600
LeaveAll Timer    10000
Dell#
```

**Related Commands**

- `garp timers` — set 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 the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

**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**

```
Dell# show gvrp brief
GVRP Feature is currently enabled.
Port                GVRP Status      Edge-Port
----------------------------------------------
Gi 3/1              Disabled          No
Gi 3/2              Enabled           No
Gi 3/3              Disabled          No
Gi 3/4              Disabled          No
Gi 3/5              Disabled          No
Gi 3/6              Disabled          No
Gi 3/7              Disabled          No
Gi 3/8              Disabled          No
Dell# show gvrp brief
```

**Related Commands**

- `show gvrp statistics` — display the GVRP statistics.

---

### show gvrp statistics

Display the GVRP configuration statistics.

**Syntax**

```
show gvrp statistics {interface interface | summary}
```

**Parameters**

- `interface interface` (OPTIONAL) Enter the keyword interface then one of the interface keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

- `summary` Enter the keyword summary to display just a summary of the GVRP statistics.
Defaults
None

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on C-Series, E-Series, and S-Series</td>
</tr>
</tbody>
</table>

Usage Information
Invalid messages/attributes skipped can occur in the following cases:
- The incoming GVRP PDU has an incorrect length.
- "End of PDU" was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.
- The attribute that was being parsed had an invalid VLAN ID. The valid range is from 1 to 4095.

A failed registration can occur for the following reasons:
- Join requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).
- An entry for a new GVRP VLAN could not be created in the GVRP database.

Example
Dell# show gvrp statistics int gi 1/1
Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
Dell#

Related Commands
- show gvrp — display the GVRP configuration.
High Availability (HA)

High availability (HA) in the Dell Networking OS is the configuration synchronization to minimize recovery time in the event of a route processor module (RPM) failure.

In general, a protocol is defined as “hitless” in the context of an RPM failure/failover and not failures of a line card, SFM, or power module. A protocol is defined as hitless if an RPM failover has no impact on the protocol.

You must specifically enable some protocols for HA. Some protocols are only hitless if related protocols are also enabled as hitless (for example, using the redundancy protocol command).

Topics:
- patch flash://RUNTIME_PATCH_DIR
- process restartable
- redundancy auto-failover-limit
- redundancy disable-auto-reboot
- redundancy force-failover
- redundancy primary
- redundancy protocol
- redundancy reset-counter
- redundancy sfm standby
- redundancy synchronize
- show patch
- show processes restartable
- show redundancy

**patch flash://RUNTIME_PATCH_DIR**

Insert an In-Service Modular Hot-Fix patch.

**Syntax**

```plaintext
patch flash://RUNTIME_PATCH_DIR/patch-filename
```

To remove the patch, use the no `patch flash://RUNTIME_PATCH_DIR/patch-filename` command.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Usage Information

The patch filename includes the Dell Networking OS version, the platform, the CPU, and the process it affects (FTOS-platform-cpu-process-patchversion.rtp). For example, a patch labeled “7.8.1.0-EH-rp2-l2mgr-1.rtp” identifies that this patch applies to Dell Networking OS version 7.8.1.0 — E-Series platform, for RP2, addressing the layer 2 management process, and this patch is the first version of this patch.

There is no need to reload or reboot the system when you insert the patch. The In-Service Modular patch replaces the existing process code. After installation is complete, the system executes the patch code as though it was always there.

### Related Commands

- `show patch` — display the system patches loaded with the in-service modular hot fix command.

### process restartable

Enable a process to be restarted. Restartability is subject to a maximum restart limit. This limit is defined as a configured number of restarts within a configured amount of time. On the software exception that exceeds the limit, the system reloads (for systems with a single RPM) or fails over (for systems with dual RPMs).

#### Syntax

```
process restartable [process] [count number] [period minutes]
```

#### Parameters

- **process**: Configure a process to be restartable.
- **count number**: Enter the number of times a process can restart within the configured period. The range is from 1 to 3. The default is 3.
- **period minutes**: Enter the amount of time within which the process can restart count times. The range is from 1 to 60 minutes. The default is 60 minutes.

#### Default

By default, a process can be restarted a maximum of three times within one hour. On the exception that exceeds this limit, the system reloads or fails over.

#### 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

- **9.8(0.0P5)**: Introduced on the S4048-ON.
- **9.8(0.0P2)**: Introduced on the S3048-ON.
- **8.3.19.0**: Introduced on the S4820T.
- **8.3.12.0**: Introduced on the S4810.
- **8.2.1.0**: Introduced.
Version Description
8.3.12.0 Introduced on the S4810.
8.4.1.0 Introduced on the E-Series.

Related Commands
- `show processes restartable` — display processes and tasks configured for restartability.

redundancy auto-failover-limit

Specify an auto-failover limit for RPMs. When a non-recoverable fatal error is detected, an automatic RPM failover occurs. This command does not affect user-initiated (manual) failovers.

Syntax
```
redundancy auto-failover-limit [count number [period minutes] | period minutes]]
```

To disable the auto-failover limit control, use the `no redundancy auto-failover-limit` command.

Parameters
- **count number**
  - Enter the number of times the RPMs can automatically failover within the period defined in the period parameter. The range is from 2 to 10. The default is 3.
- **period minutes**
  - Enter a duration in which to allow a number of automatic failovers (limited to the number defined in the count parameter). The range is from 5 to 9000 minutes. The default is 60 minutes.

Default
- Count: 3
- Period: 60 minutes

Command Modes
- `CONFIGURATION`

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

Usage Information
If you disable auto failover, enter the `redundancy auto-failover-limit` (without any parameters) to set auto failover to the default parameters (Count 3, Period 60 minutes). To view the redundancy status, use the `show redundancy` command.
When you change one or both of the optional parameters, Dell Networking OS checks that the interval between auto failovers is more than five (5) minutes. If the interval is less, Dell Networking OS returns a configuration error message.

**redundancy disable-auto-reboot**

Prevent the system from auto-rebooting the failed module.

**Syntax**

```
redundancy disable-auto-reboot stack-unit [stack-unit ID| members} [rpm| card number | all]
To return to the default, use the no redundancy disable-auto-reboot stack-unit rpm command.
```

**Parameters**

- `rpm` Enter the keyword `rpm` to disable auto-reboot of the failed RPM.
- `stack-unit` Enter the keyword `stack-unit` then the stack-unit ID number.

**Default**

Disabled — the failed module is automatically rebooted.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the <code>all</code> option.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series</td>
</tr>
</tbody>
</table>

**Usage Information**

Enabling this command keeps the failed RPM in the failed state. If there are two RPMs in the system, enabling this command prevents the failed RPM from becoming a working Standby RPM. If there is only one RPM in the system, the failed RPM does not recover and affects the system.
**redundancy force-failover**

Force the secondary stack unit to become the primary stack unit. You can also use this command to upgrade the software on one stack unit from the other when the other has been loaded with the upgraded software.

**Syntax**

redundancy force-failover stack-unit

**Parameters**

- **stack-unit**
  
Enter the keyword stack-unit then the stack-unit ID number.

**Default**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(10)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To provide a hitless or warm upgrade, use this command. A hitless upgrade means that a software upgrade does not require a reboot of the line cards. A warm upgrade means that a software upgrade requires a reset of the line cards. A warm upgrade is possible for major releases and lower, while a hitless upgrade can only support patch releases.

**redundancy primary**

Set an RPM as the primary RPM.

**Syntax**

redundancy primary [rpm0 | rpm1]

To delete a configuration, use the no redundancy primary command.
Parameters

- **rpm0**
  Enter the keyword rpm0 to set the RPM in slot R0 as the primary RPM.

- **rpm1**
  Enter the keyword rpm1 to set the RPM in slot R1 as the primary RPM.

Default

The RPM in slot R0 is the Primary RPM.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---

**redundancy protocol**

Enable hitless protocols.

Syntax

```
redundancy protocol {lacp | xstp}
```

To disable a hitless protocol, use the `no redundancy protocol {lacp | xstp}` command.

Parameters

- **lacp**
  Enter the keyword lacp to make LACP hitless.

- **xstp**
  Enter the keyword xstp to invoke hitless STP (all STP modes — MSTP, PVST+, RSTP, and STP).

Default

Disabled

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
8.3.7.0 | Introduced on the S4810.
8.2.1.0 | Introduced on the C-Series.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the E-Series.

Related Commands
- `show lacp` — display the lacp configuration.
- `show redundancy` — display the current redundancy configuration.

**redundancy reset-counter**

Reset failover counter and timestamp information displayed in the `show redundancy` command.

**Syntax**

```
redundancy reset-counter
```

**Default**

Not configured.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**redundancy sfm standby**

Place the SFM in an offline state.

**Syntax**

```
redundancy sfm standby
```

To place the SFM in an online state, use the `no redundancy sfm standby` command.
The SFM is online by default.

**Command Modes**
- CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
When you insert or remove a secondary RPM with logical SFM, the system must add or remove the backplane links to the switch fabric trunk. To avoid traffic disruption, use this command when you insert the secondary RPM. When you execute this command, the logical SFM on the standby RPM is immediately taken offline and the SFM state is set as "standby".

**NOTE:** This command could affect traffic when taking the secondary SFM offline.

**Example**
```
Dell# show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot Status
--------------------------------------
0    active
1    active

Dell# configure
Dell(conf)# redundancy sfm standby
Taking secondary SFM offline...
!
Dell(conf)# do show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot Status
-----------------------------------------
0    active
1    standby

Dell(conf)# no redundancy sfm
Taking secondary SFM online...
!
Dell(conf)# do show sfm all
Switch Fabric State: up
-- Switch Fabric Modules --
Slot Status
-------------------------------------------
0    active
1    active
```
redundancy synchronize

Manually synchronize data once between the Master and Stand-by stack units.

Syntax

redundancy synchronize [full]

Parameters

full Enter the keyword full to synchronize all data.

Default

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

show patch

Display the system patches loaded with the In-Service Modular Hot Fix command.

Syntax

show patch

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
show processes restartable

Display the processes and tasks configured for restartability.

Syntax

show processes restartable [history]

Parameters

history Display the last time the restartable processes crashed.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.4.1.0 Introduced on the E-Series.

Example

Dell# show processes restartable
---------------------------------------------
Process name State How many times restarted Timestamp last restarted
---------------------------------------------
radius enabled 0 [-]
tacplus enabled 0 [-]
---------------------------------------------
Dell# show processes restartable history
---------------------------------------------
Process name Timestamp last crashed
---------------------------------------------
---------------------------------------------

Related Commands

- process restartable — enable a process to restart.
**show redundancy**

Display the current redundancy configuration.

**Syntax**

```
show redundancy
```

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show redundancy` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPM Status</td>
<td>Displays the following information:</td>
</tr>
<tr>
<td></td>
<td>- Slot number of the RPM.</td>
</tr>
<tr>
<td></td>
<td>- Whether the RPM is Primary or Standby.</td>
</tr>
<tr>
<td></td>
<td>- The state of the RPM: Active, Standby, Booting, or Offline.</td>
</tr>
<tr>
<td></td>
<td>- Whether the link to the second RPM is up or down.</td>
</tr>
<tr>
<td>PEER RPM Status</td>
<td>Displays the state of the second RPM, if present</td>
</tr>
<tr>
<td>RPM Redundancy</td>
<td>Displays the following information:</td>
</tr>
<tr>
<td>Configuration</td>
<td>- which RPM is the preferred Primary on next boot (the <code>redundancy primary</code> command)</td>
</tr>
<tr>
<td></td>
<td>- the data sync method configured (the <code>redundancy synchronize</code> command)</td>
</tr>
</tbody>
</table>
|                        | - the failover type (you cannot change this type; it is software-dependent). Hot Failover means that the running configuration and routing table are applied on secondary RPM. Fast Failover means that the running configuration is not applied on
Field Description

- the secondary RPM until failover occurs, and the routing table on line cards is cleared during failover.
- the status of auto booting the RPM (the `redundancy disable-auto-reboot` command)
- the parameter for auto failover limit control (the `redundancy auto-failover-limit` command)

RPM Failover Record
Displays the following information:
- RPM failover counter (to reset the counter, use the `redundancy reset-counter` command)
- the time and date of the last RPM failover
- the reason for the last RPM failover

Last Data Sync Record
Displays the data sync information and the timestamp for the data sync:
- Start-up Config is the contents of the `startup-config` file.
- Line Card Config is the line card types configured and interfaces on those line cards.
- Runtime Event Log is the contents of the Event log.
- Running Config is the current `running-config`.

This field only appears when you enter the command from the Primary RPM.

Example

Dell# show redundancy
-- RPM Status --
-----------------------------------------------
RPM Slot ID: 1
RPM Redundancy Role: Primary
RPM State: Active
RPM SW Version: 7.5.1.0
Link to Peer: Up
-- PEER RPM Status --
-----------------------------------------------
RPM State: Standby
RPM SW Version: 7.5.1.0
-- RPM Redundancy Configuration --
-----------------------------------------------
Primary RPM: rpm0
Auto Data Sync: Full
Failover Type: Hot Failover
Auto reboot RPM: Enabled
Auto failover limit: 3 times in 60 minutes
-- RPM Failover Record --
-----------------------------------------------
Failover Count: 1
Last failover timestamp: Jul 13 2007 21:25:32
Last failover Reason: User request
-- Last Data Block Sync Record: --
-----------------------------------------------
Dell#
ICMP Message Types

This section lists and describes the possible ICMP message type resulting from a ping. The first three columns list the possible symbol or type/code. For example, you would receive a ! or 03 as an echo reply from your ping.

ICMP Messages and their Definitions.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
<th>Query</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>0</td>
<td>3</td>
<td>echo reply</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>!</td>
<td>0</td>
<td>3</td>
<td>destination unreachable:</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>3</td>
<td></td>
<td>network unreachable</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>0</td>
<td></td>
<td>host unreachable</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>1</td>
<td></td>
<td>protocol unreachable</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>2</td>
<td></td>
<td>port unreachable</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>3</td>
<td></td>
<td>fragmentation needed but don’t fragment bit set</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>4</td>
<td></td>
<td>source route failed</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>5</td>
<td></td>
<td>destination network unknown</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>6</td>
<td></td>
<td>destination host unknown</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>7</td>
<td></td>
<td>source host isolated (obsolete)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>8</td>
<td></td>
<td>destination network administratively prohibited</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>9</td>
<td></td>
<td>destination host administratively prohibited</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>10</td>
<td></td>
<td>network unreachable for TOS</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>11</td>
<td></td>
<td>host unreachable for TOS</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>12</td>
<td></td>
<td>communication administratively prohibited by filtering</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>13</td>
<td></td>
<td>host precedence violation</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>U</td>
<td>14</td>
<td></td>
<td>precedence cutoff in effect</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>4</td>
<td>0</td>
<td>source quench</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>5</td>
<td></td>
<td>redirect</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td></td>
<td>redirect for network</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>1</td>
<td></td>
<td>redirect for host</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td></td>
<td>redirect for type-of-service and network</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td></td>
<td>redirect for type-of-service and host</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
<td>0</td>
<td>echo request</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>9</td>
<td>0</td>
<td>router advertisement</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>C</td>
<td>10</td>
<td>0</td>
<td>router solicitation</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td>Symbol</td>
<td>Type</td>
<td>Code</td>
<td>Description</td>
<td>Query</td>
<td>Error</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>------</td>
<td>--------------------------------------------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>&amp;</td>
<td>11</td>
<td>0</td>
<td>time-to-live equals 0 during transit</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>time-to-live equals 0 during reassembly</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>1</td>
<td>parameter problem:</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>IP header bad (catchall error)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>0</td>
<td>timestamp request</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>0</td>
<td>timestamp reply</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>0</td>
<td>information request (obsolete)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>0</td>
<td>information reply (obsolete)</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>0</td>
<td>address mask request</td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>0</td>
<td>address mask reply</td>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>
Internet Group Management Protocol (IGMP)

The IGMP commands are supported on the Dell Networking OS.

Topics:

- IGMP Commands
- IGMP Snooping Commands

IGMP Commands

Dell Networking OS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- Dell Networking OS supports protocol-independent multicast-sparse (PIM-SM) and protocol-independent source-specific multicast (PIM-SSM) include and exclude modes.
- IGMPv2 is the default version of IGMP on interfaces. You can configure IGMPv3 on interfaces. It is backward compatible with IGMPv2.
- The maximum number of interfaces supported is 95.
- There is no hard limit on the maximum number of groups supported.
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
- An administrative command (ip igmp version) is added to manually set the IGMP version.
- All commands previously used for IGMPv2 are compatible with IGMPv3.

clear ip igmp groups

Clear entries from the group cache table.

Syntax

```plaintext
clear ip igmp [vrf vrf-name] groups [group-address | interface]
```

Parameters

- **vrf vrf-name**  
  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.
  
  **NOTE:** Applies to specific VRF if input is provided, else applies to default VRF.

- **group-address**  
  (OPTIONAL) Enter the IP multicast group address in dotted decimal format.

- **interface interface**  
  Enter the following keywords and the interface information:
  
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes**

| EXEC |

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td><strong>E-Series legacy command</strong></td>
<td></td>
</tr>
</tbody>
</table>

**debug ip igmp**

Enable debugging of IGMP packets.

**Syntax**

```
ddebug ip igmp [vrf vrf-name] [group address | interface]
```

- To disable IGMP debugging, use the `no debug ip igmp [vrf vrf-name] [group address | interface]` command.
- To disable all debugging, use the `undebug all` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to enable</td>
</tr>
<tr>
<td></td>
<td>debugging of IGMP packets corresponding to that VRF.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to specific VRF if input is provided, else applies to Default</td>
</tr>
<tr>
<td></td>
<td>VRF.</td>
</tr>
<tr>
<td>group-address</td>
<td>(OPTIONAL) Enter the IP multicast group address in dotted decimal format.</td>
</tr>
</tbody>
</table>
**interface interface**

Enter the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.

**Defaults**

Disabled.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Usage Information**

IGMP commands accept only non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

**ip igmp access-group**

To specify access control for packets, use this feature.

**Syntax**

```
ip igmp access-group access-list
```

To remove the feature, use the `no ip igmp access-group access-list` command.
Parameters

access-list
   Enter the name of the extended ACL (16 characters maximum).

Defaults

Not configured

Command Modes

INTERFACE (conf-if-interface-slot/port)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The access list accepted is an extended ACL. To block IGMP reports from hosts, on a per-interface basis based on the group address and source address that you specify in the access list, use this feature.

**ip igmp immediate-leave**

Enable IGMP immediate leave.

Syntax

```
ip igmp immediate-leave [group-list prefix-list-name]
```

To disable `ip igmp immediate-leave`, use the `no ip igmp immediate-leave` command.

Parameters

- `group-list prefix-list-name`
  - Enter the keywords `group-list` then a string up to 16 characters long of the prefix-list-name.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Querier normally sends some group-specific queries when a leave message is received for a group prior to deleting a group from the membership database. There may be situations when you require immediate deletion of a group from the membership database. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable immediate-leave processing for specified groups.

**ip igmp last-member-query-interval**

Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

**Syntax**

```
ip igmp last-member-query-interval milliseconds
```

To return to the default value, use the `no ip igmp last-member-query-interval` command.

**Parameters**

- `milliseconds` Enter the number of milliseconds as the interval. For IGMP version 2, the range is from 100 to 25599. For IGMP version 3, the range is from 100 to 65535. The default value is 1000 milliseconds.

**Defaults**

1000 milliseconds

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

- **E-Series legacy command**
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Maximum range of the Hello interval value is changed to 18000. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

`ip igmp query-interval`  

Change the transmission frequency of IGMP general queries the Querier sends.

**Syntax**

```
ip igmp query-interval seconds
```

To return to the default values, use the **no** `ip igmp query-interval` command.

**Parameters**

- `seconds`  
  Enter the number of seconds between queries sent out. The range is from 1 to 18000. The default is **60 seconds**.

**Defaults**

- **60 seconds**

**Command Modes**

- INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Maximum range of the Hello interval value is changed to 18000. Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
Version                  Description
9.5(0.0)                 Introduced on the Z9500.
9.2(0.0)                 Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0                  Introduced on the S6000.
8.3.19.0                 Introduced on the S4820T.
8.3.11.1                 Introduced on the Z9000.
8.3.7.0                  Introduced on the S4810.
7.8.1.0                  Introduced on the S-Series.
7.7.1.0                  Introduced on the C-Series.
7.6.1.0                  Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0                  Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

E-Series legacy command.

Usage Information
If you have configured the hello interval value to be greater than 18000, you must first reset that value to be less than or equal to 18000 before upload. Otherwise, the command execution fails during bootup and the hello interval value is set to the default value.

**ip igmp query-max-resp-time**

Set the maximum query response time advertised in general queries.

**NOTE:** The IGMP query-max-resp-time value must be less than the IGMP query-interval value.

**Syntax**

```plaintext
ip igmp query-max-resp-time seconds
```

To return to the default values, use the

```plaintext
no ip igmp query-max-resp-time command.
```

**Parameters**

- `seconds`
  
Enter the number of seconds for the maximum response time. The range is from 1 to 25. The default is **10 seconds**.

**Defaults**

**10 seconds**

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**                  **Description**
9.10(0.0)                   Introduced on the S6100–ON.
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.
ip igmp ssm-map

To translate (*,G) memberships to (S,G) memberships, use a statically configured list.

Syntax

```
ip igmp [vrf vrf-name] ssm-map std-access-list source-address
```

Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) state, use the `ip igmp [vrf vrf-name] ssm-map std-access-list source-address` command.

Parameters

- **vrf vrf-name**
  - (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.
  - **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- **std-access-list**
  - Specify the standard IP access list that contains the mapping rules for multicast groups.

- **source-address**
  - Specify the multicast source address to which the groups are mapped.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100-ON.

9.8(1.0) Introduced on the Z9100-ON.

7.6.1.0 Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

7.6.1.0 Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

E-Series legacy command.

Version Description

9.5(0.0) Introduced on the Z9500.

9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

7.5.1.0 Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

7.5.1.0 Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

Internet Group Management Protocol (IGMP)
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF and introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information
Mapping applies to both v1 and v2 IGMP joins; any updates to the ACL are reflected in the IGMP groups. You may not use extended access lists with this command. When you configure a static SSM map and the router cannot find any matching access lists, the router continues to accept (*,G) groups.

### Related Commands
- `ip access-list standard` — create a standard access list to filter based on IP address.

---

### ip igmp version
Manually set the version of the router to IGMPv2 or IGMPv3.

**Syntax**
```
ip igmp version {2 | 3}
```

**Parameters**
- `2` Enter the number 2 to set the IGMP version number to IGMPv2.
- `3` Enter the number 3 to set the IGMP version number to IGMPv3.

**Defaults**
2 (IGMPv2)

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Changed the default IGMP from version 2 to version 3. Introduced on the S6000-ON</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
show ip igmp groups

View the IGMP groups.

Syntax
show ip igmp [vrf vrf-name] groups [group-address [detail] | detail | interface [group-address [detail]]]

Parameters
vrf vrf-name (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.

group-address (OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.

interface (OPTIONAL) Enter the interface type and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

detail (OPTIONAL) Enter the keyword detail to display the IGMPv3 source information.

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Added support for VRF. Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series and C-Series.
7.5.1.0 | Expanded to support the detail option.

**E-Series legacy command.**

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Lists the multicast address for the IGMP group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Lists the interface type, slot and port number.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the IGMP version used.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the amount of time the group has been operational.</td>
</tr>
<tr>
<td>Expires</td>
<td>Displays the amount of time until the entry expires.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>Displays the IP address of the last host to be a member of the IGMP group.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Uptime Expires
225.0.0.0    Vlan 100   00:00:05 00:02:04
225.0.0.1    Vlan 100   00:00:05 00:02:04
225.0.0.2    Vlan 100   00:00:05 00:02:04
225.0.0.3    Vlan 100   00:00:05 00:02:04
225.0.0.4    Vlan 100   00:00:05 00:02:04
```

**Example (VLT)**

```
NOTE: The asterisk (*) after the port channel number (Po 2) highlighted in the following example indicates the port channel is VLT, that the local VLT port channel is down and the remote VLT port is up.
```
show ip igmp interface

View information on the interfaces participating in IGMP.

Syntax

show ip igmp [vrf vrf-name] interface [interface]

Parameters

vrf vrf-name 

(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to view IGMP interfaces associated with that VRF.

interface 

(OPTIONAL) Enter the interface type and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.
## Version Description

9.8(1.0)  Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)  Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)  Introduced on the Z9500.
9.0.2.0  Introduced on the S6000.
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.3.7.0  Introduced on the S4810.
7.6.1.0  Introduced on the S-Series.
7.5.1.0  Introduced on the C-Series.

**E-Series legacy command.**

### Usage Information

IGMP commands accept only non-VLAN interfaces — specifying VLAN does not yield results.

The `show ip igmp interface` command does not display information corresponding to the loop-back interfaces.

### Example

```
Dell# show ip igmp interface
GigabitEthernet 1/1 is down, line protocol is down
   Internet protocol processing disabled
GigabitEthernet 1/5 is down, line protocol is down
   Internet protocol processing disabled
GigabitEthernet 1/6 is down, line protocol is down
   Internet protocol processing disabled
GigabitEthernet 1/7 is up, line protocol is down
   Internet protocol processing disabled
Vlan 20
   Inbound IGMP access group is not set
   Internet address is 35.0.0.1/24
   IGMP is enabled on interface
   IGMP query interval is 60 seconds
   IGMP querier timeout is 125 seconds
   IGMP max query response time is 10 seconds
   IGMP last member query response interval is 1000 ms
   IGMP immediate-leave is enabled for all groups
   IGMP activity: 0 joins
   IGMP querying router is 35.0.0.1 (this system)
   IGMP version is 2
```

### Example (VRF)

```
Dell# show ip igmp vrf BLUE interface
GigabitEthernet 1/20
   Inbound IGMP access group is not set
   Internet address is 50.10.4.1/24
   IGMP is up on the interface
   IGMP query interval is 60 seconds
   IGMP querier timeout is 0 seconds
   IGMP max query response time is 10 seconds
   IGMP last member query response interval is 1000 ms
   IGMP immediate-leave is enabled for all groups
   IGMP activity: 0 joins
   IGMP querying router is 50.10.4.1 (this system)
   IGMP version is 3
Vlan 4007
   Inbound IGMP access group is not set
```
show ip igmp ssm-map

Display is a list of groups that are currently in the IGMP group table and contain SSM mapped sources.

Syntax

```
show ip igmp [vrf vrf-name] ssm-map [group]
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.
  
  **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- `group` (OPTIONAL) Enter the multicast group address in the form A.B.C.D to display the list of sources to which this group is mapped.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>
IGMP Snooping Commands

Dell Networking OS supports IGMP Snooping version 2 and 3 on all Dell Networking systems.

Important Points to Remember for IGMP Snooping

- Dell Networking OS supports version 1, version 2, and version 3 hosts.
- Dell Networking OS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- Dell Networking OS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- Dell Networking OS supports IGMP snooping on JUMBO-enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.
- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes multiple spanning tree protocol (MSTP) triggers by sending a general query on the interface that comes in the FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is reassigned to the VLAN interface.
- When enabled, IGMP snooping Querier does not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it checks the IP source address of the incoming frame.
If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, the switch disables its IGMP snooping Querier functionality.

If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch continues to work as an IGMP snooping Querier.

clear ip igmp snooping groups

Clear snooping entries from the group cache table.

Syntax

```
clear ip igmp snooping groups [group-address interface | interface]
```

Parameters

- **group-address** (OPTIONAL) Enter the IP multicast group address in dotted decimal format.
- **interface interface** Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.

Command Modes

- EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

Usage Information

IGMP commands accept only non-VLAN interfaces — specifying VLAN does not yield results.

debug ip igmp snooping

Enable debugging of IGMP snooping packets on interfaces and groups.

Syntax

```
debug ip igmp snooping [group address | interface]
```

To disable debugging of IGMP snooping, use the no debug ip igmp snooping [group address | interface] command.
• To disable all debugging, use the `undo debug all` command.

**Parameters**

- `snooping`
  - Enter the keyword `snooping` to enable debugging of IGMP snooping.
- `group-address`
  - *OPTIONAL* Enter the IP multicast group address in dotted decimal format.
- `interface interface`
  - Enter the following keywords and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a port channel interface, enter the keywords `port-channel` then a number.

**Defaults**

Disabled.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, Z9000, and Z9500.</td>
</tr>
</tbody>
</table>

**Usage Information**

IGMP commands accept only non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

**ip igmp snooping enable**

Enable IGMP snooping on all or a single VLAN. This command is the master on/off switch to enable IGMP snooping.

**Syntax**

```
ip igmp snooping enable
```

To disable IGMP snooping, use the `no ip igmp snooping enable` command.

**Defaults**

Disabled.

**Command Modes**

- CONFIGURATION
- INTERFACE VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
</tbody>
</table>
### Version Description

- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.5(0.1)** Introduced on the Z9500.
- **9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.7.0** Introduced on the S4810.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.

### Usage Information

To enable IGMP snooping, enter this command. When you enable this command from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN).

> **NOTE:** Execute the no shutdown command on the VLAN interface for IGMP Snooping to function.

### ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

**Syntax**

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the no igmp snooping fast-leave command.

**Defaults**

Not configured.

**Command Modes**

INTERFACE VLAN — (conf-if-vl-

**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.
- **9.8(1.0)** Introduced on the Z9100–ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.5(0.1)** Introduced on the Z9500.
- **9.2(0.0)** Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
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.

**Syntax**

```
ip igmp snooping flood
```

To undo this configuration, use the `no ip igmp snooping flood` command.

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command.
Usage Information

On the C-Series and S-Series, unregistered multicast data traffic drops when you disable flooding; they do not forward the packets to multicast router ports. On the C-Series and S-Series, in order to disable Layer 2 multicast flooding, disable Layer 3 multicast (no ip multicast-routing).

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

Syntax

ip igmp snooping last-member-query-interval milliseconds

To return to the default value, use the no ip igmp snooping last-member-query-interval command.

Parameters

milliseconds Enter the interval in milliseconds. The range is from 100 to 65535. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.

9.8(1.0) Introduced on the Z9100–ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.5(0.1) Introduced on the Z9500.

9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

E-Series legacy command
Usage Information

This last-member-query-interval is also the interval between successive Group-Specific Query messages. To change the last-member-query interval, use this command.

**ip igmp snooping mrouter**

Statically configure a VLAN member port as a multicast router interface.

**Syntax**

```plaintext
ip igmp snooping mrouter interface interface
```

To delete a specific multicast router interface, use the `no igmp snooping mrouter interface interface` command.

**Parameters**

- **interface interface**
  
  Enter the following keywords and the interface information:
  
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

**Defaults**

Not configured.

**Command Modes**

INTERFACE VLAN — (conf-if-vl-)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
The Dell Networking OS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

### ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

**Syntax**

```
ip igmp snooping querier
```

To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.

**Defaults**

Not configured.

**Command Modes**

INTERFACE VLAN — (conf-if-vl-n)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command
This command enables the IGMP switch to send General Queries periodically. This behavior is useful when there is no multicast router present in the VLAN because the multicast traffic is not routed. Assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

**show ip igmp snooping groups**

Display snooping related information for all the IGMP groups, interface or one group of one interface.

**Syntax**

```
show ip igmp snooping groups [group-address [detail] | detail | interface [group-address [detail]]]
```

**Parameters**

- `snooping` Enter the keyword `snooping` to display snooping related information.
- `group-address` (OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
- `interface` (OPTIONAL) Enter the interface type and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- `detail` (OPTIONAL) Enter the keyword `detail` to display the IGMPv3 source information.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the following example.
### Field Description
- **Group Address**: Lists the multicast address for the IGMP group.
- **Interface**: Lists the interface type, slot and port number.
- **Mode**: Displays the IGMP version used.
- **Uptime**: Displays the amount of time the group has been operational.
- **Expires**: Displays the amount of time until the entry expires.
- **Last Reporter**: Displays the IP address of the last host to be a member of the IGMP group.
- **Member Ports**: Indicates the port channel. If the port channel is VLT, an asterisk (*) after the port channel number indicates the port channel is locally down and that a remote VLT port is up.

#### Example
```plaintext
Dell# show ip igmp snooping groups
Total Number of Groups: 1
IGMP Connected Group Membership
  Group Address    Interface      Mode          Uptime    Expires   Last Reporter
  225.1.1.1        Vlan 10       IGMPv2-Compat 00:00:07 00:02:09 1.1.1.2
  Member Ports: Gi 1/17
Dell#
```

### show ip igmp snooping mrouter
Display multicast router interfaces.

#### Syntax
```plaintext
show ip igmp snooping mrouter [vlan number]
```

#### Parameters
- **vlan number**: Enter the keyword `vlan` then the vlan number. The range is from 1 to 4094.

#### Command Modes
- EXEC
- EXEC Privilege

#### Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

#### Version
- **9.10(0.0)**: Introduced on the S6100–ON.
- **9.8(1.0)**: Introduced on the Z9100–ON.
- **9.8(0.0P5)**: Introduced on the S4048-ON.
- **9.8(0.0P2)**: Introduced on the S3048-ON.
- **9.7(0.0)**: Introduced on the S6000-ON.
- **9.5(0.1)**: Introduced on the Z9500.
- **9.0.2.0**: Introduced on the S6000.
- **8.3.19.0**: Introduced on the S4820T.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command.**

**Usage Information**
If the port channel is a VLT port channel, an asterisk (*) after the port channel number (Po 100*) indicates the port channel is locally down and that a remote VLT port is up.

**Example**
```
Dell# show ip igmp snooping mrouter
Interface Router Ports
Vlan 2 Gi 1/3, Po 1
Dell#
```

**Related Commands**
- `ip igmp snooping mrouter` — configure a static connection to the multicast router.
- `show ip igmp groups` — view groups.
To configure egress, port channel, time domain, and UDP, use these interface commands.

Topics:
- Basic Interface Commands
- Egress Interface Selection (EIS) Commands
- Port Channel Commands
- Time Domain Reflectometer (TDR) Commands
- UDP Broadcast Commands

## Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

### clear counters

Clear the counters displayed in the show interfaces commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

**Syntax**

```
clear counters [interface | vrrp {vr-id | ipv6 vr-id} | learning-limit | vlan vlan-id]
```

**Parameters**

- **interface**
  
  (OPTIONAL) Enter any of the following keywords and the interface information to clear counters from a specified interface:

  - For IPv4 access-group counters, enter the keyword `ip`.
  - For IPv6 access-group counters, enter the keyword `ipv6`.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For MAC access-group counters, enter the keyword `mac`.
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - For the management interface, enter the keyword `ManagementEthernet` then slot/port information.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a tunnel interface, enter the keyword `tunnel`. The range is from 1 to 16383.

**NOTE:** This command also enables you to clear the port configurations 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 clear the port configurations 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 clear the port configurations corresponding to all ports between 1 and 4, specify the port range as show interfaces interface-type 1/1/1 - 1/1/4.

```
vrrp [ipv6 {vr-id} | vr-id]

learning-limit

vlan vlan-id
```

(OPTIONAL) Enter the keyword vrrp to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter ipv6. To clear the counters of a specified group, enter a VRID number from 1 to 255.

(OPTIONAL) Enter the keywords learning-limit to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

Enter the keyword vlan followed by the interface VLAN number. The range is from 1 to 4094.

Defaults

Without an interface specified, the command clears all interface counters.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to clear the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support (E-Series only) for VRRP groups in a VRF instance.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4093 VLANs on the E-Series. Prior to the release, 2094 was supported.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Updated the definition of the learning-limit option for clarity.</td>
</tr>
</tbody>
</table>
Example
Dell# clear counters
Clear counters on all interfaces [confirm]
Dell#

Related Commands
- mac learning-limit — allow aging of MACs even though a learning-limit is configured or disallow station move on learned MACs.
- show interfaces — display information on the interfaces.

clear dampening
Clear the dampening counters on all the interfaces or just the specified interface.

Syntax
clear dampening [interface]

Parameters
- interface (OPTIONAL) Enter any of the following keywords and the interface information to clear counters from a specified interface:
  - For a Port Channel interface, enter the keywords port-channel then a number.
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Defaults
Without an interface specified, the command clears all interface dampening counters.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
dampening

Configure dampening on an interface.

Syntax
dampening [[[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]

Parameters

- **half-life**: Enter the number of seconds after which the penalty is decreased. The penalty decreases half after the half-life period expires. The range is from 1 to 30 seconds. The default is 5 seconds.

- **reuse-threshold**: Enter a number as the reuse threshold, the penalty value below which the interface state is changed to "up". The range is from 1 to 20000. The default is 750.

- **suppress-threshold**: Enter a number as the suppress threshold, the penalty value above which the interface state is changed to "error disabled". The range is from 1 to 20000. The default is 2500.

- **max-suppress-time**: Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. The range is from 1 to 86400. The default is 20 seconds.

Defaults

Disabled.

Command Modes

INTERFACE (conf-if-)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
------- | -----------
9.10(0.0) | Introduced on the S6100–ON.
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.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.
## Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

With each flap, Dell Networking OS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface moves to the Error-Disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. After the penalty decays below the reuse threshold, the interface enables. The configured parameters are as follows:

- suppress-threshold should be greater than reuse-threshold
- max-suppress-time should be at least 4 times half-life

**NOTE:** You cannot apply dampening on an interface that is monitoring traffic for other interfaces.

### Example

```bash
Dell(conf-if-gi-1/10)# dampening 20 800 4500 120
Dell(conf-if-gi-1/10)#
```

### Related Commands

- `clear dampening` — clear the dampening counters on all the interfaces or just the specified interface.
- `show interfaces dampening` — display interface dampening information.

---

### default interface

Reset a physical interface to its factory default settings.

#### Syntax

```bash
default interface interface-type slot/port - range
```

#### Parameters

- **interface-type slot/port**
  - Enter the interface type and slot/port information:
    - For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- **range**
  - 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 - 1/1/4`.

#### Defaults

None

#### Command Modes

- CONFIGURATION

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**Version**  
9.9(0.0)  
Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, and Z9500.

**Usage Information**  
Use the `default interface` command to set a Gigabit Ethernet, 10- Gigabit Ethernet, or 40-Gigabit Ethernet interface to its factory-default state. By default, a physical interface is disabled (shutdown) with no assigned IP address or switchport (no ip address). This command removes all software settings and all L3, VLAN, VXLAN, and port-channel configurations on a physical interface.

**Example**  
```
Dell(conf-if-gi-1/5)# show config
!
interface GigabitEthernet 1/5
  description testconfig
  no ip address
  portmode hybrid
  switchport
  rate-interval 8
  mac learning-limit 10 no-station-move
  no shutdown
Dell(conf-if-gi-1/5)#

Dell(conf)# default interface gigabitethernet 1/5

Dell(conf-if-gi-1/5)# show config
!
interface GigabitEthernet 1/5
  no ip address
  shutdown
```

**Related Commands**  
- `show running-config` – display the current configuration.

---

**description**

Assign a descriptive text string to the interface.

**Syntax**  
```
description desc_text
```

To delete a description, use the `no description` command.

**Parameters**  
- `desc_text`  
Enter a text string up to 240 characters long.

**Defaults**  
None

**Command Modes**  
INTERF ACE

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**  
9.10(0.0)  
Introduced on the S6100–ON.

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.
### Interfaces

#### duplex (10/100 Interfaces)

Configure duplex mode on the Management Interface interfaces where the speed is set to 10/100.

**Syntax**

```
duplex full
```

To return to the default setting, use the `no duplex` command.

**Parameters**

- **full**: Enter the keyword `full` to set the physical interface to transmit in both directions.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
**Version** | **Description**
--- | ---
9.7(0.0) | Introduced on the S6000-ON.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.4.1.0 | Introduced

**Usage Information**
This command applies to any physical interface with speed set to 10/100.

**NOTE:** Starting with Dell Networking OS version 7.8.1.0, when you use a copper SFP2 module with catalog number GP-SFP2-1T in the S25P model of the S-Series, you can manually set its speed with the `speed` command. When you set the speed to 10 Mbps or 100 Mbps, you can also execute the `duplex` command.

**Related Commands**
- `negotiation auto` — enable or disables auto-negotiation on an interface.

---

### flowcontrol

Control how the system responds to and generates 802.3x pause frames.

**Syntax**
```
flowcontrol rx {off | on} tx {off | on} [negotiate | pause-threshold value | resume-offset value]
```

To return to the default, use the `no` form of this command.

**Parameters**
- `rx on` | Enter the keywords `rx on` to process the received flow control frames on this port.
- `rx off` | Enter the keywords `rx off` to ignore the received flow control frames on this port.
- `tx on` | Enter the keywords `tx on` to send control frames from this port to the connected device when a higher rate of traffic is received.
- `tx off` | Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.
- `pause-threshold` | Enter the buffer threshold limit for generating PAUSE frames.
- `resume-offset` | Enter the offset value for generating PAUSE frames to resume traffic.

**Defaults**

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version | Description
--- | ---
9.10(0.0) | Introduced on the S6100-ON.
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
6.5.1.9 and 7.4.1.0 | Introduced on the E-Series.
7.8.1.0 | Introduced on the C-Series and S-Series with the thresholds option.

**Usage Information**
The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

When a port receives traffic at a higher rate than it can process, the frames are stored in the port buffer. As a result, buffer usage increases. When the buffer usage reaches the value specified in the "pause-threshold" argument, the port sends PAUSE frame to the connected link partner to stop sending the traffic. Eventually this reduces the buffer usage. When the buffer usage drops by the value specified in the "resume-threshold", the port again sends a PAUSE frame with 0 as wait-time. This results in resume of the paused traffic flow.

**Important Points to Remember**
- Do not enable tx pause when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Speeds less than 1 Gig cannot be configured when the asymmetric flow control configuration is on. The following error is returned:
  ```
  Can’t configure speed <1G when Asymmetric flowcontrol is on, config ignored
  ```
- Dell Networking OS only supports rx on tx on and rx off tx off for speeds less than 1 Gig (Symmetric).

**NOTE:** If you use the disable rx flow control command, Dell Networking recommends rebooting the system.

**Example**
```
Dell(conf-if-Gi-1/1)# show config
!
interface GigabitEthernet 1/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...```
This Example shows how Dell Networking OS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 1G copper ports.

<table>
<thead>
<tr>
<th>Configured</th>
<th>LocRxConf</th>
<th>LocTxConf</th>
<th>RemoteRxConf</th>
<th>RemoteTxConf</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>off</td>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
<td>off</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>off</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>off</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>display the flow configuration parameters (non-default values only).</td>
<td>show interfaces</td>
<td>display the negotiated flow control parameters.</td>
</tr>
</tbody>
</table>

### interface

Configure a physical or virtual interface on the switch.

**Syntax**

```
interface interface
```

**Parameters**

**interface**

Enter one of the following keywords and the interface information:

- For a null interface, enter the keyword `null` then the slot/port information. The Null interface number is 0.
- For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Tunnel interface, enter the keyword tunnel then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.
- For a port channel interface, enter the keywords port-channel then a number.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the support for interfaces.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**
You cannot delete a physical interface.

By default, physical interfaces are disabled (shutdown) and are not assigned to an IP address or switchport. To place an interface in Layer 2 mode, ensure that the interface's configuration does not contain an IP address and enter the switchport command.

You can create up to 64 tunnel interfaces. The tunnel is added as a logical interface with no default configuration. To delete a tunnel interface, use the no interface tunnel tunnel-id command.
The tunnel interface operates as an ECMP (equal cost multi path) only when the next hop to the tunnel destination is over a physical interface. If you select any other interface as the next hop to the tunnel destination, the tunnel interface does not operate as an ECMP.

Example

Dell(conf)# int tengigabitethernet 1/10
Dell(conf-if-gi-1/10)# exit
Dell(conf)#

Related Commands

- interface loopback — configure a Loopback interface.
- interface null — configure a Null interface.
- interface port-channel — configure a port channel.
- interface vlan — configure a VLAN.
- show interfaces — display the interface configuration.

interface group

Create or delete group of VLANs with a single command. You can also use this command to apply a set of configurations on a group of interfaces.

Syntax

interface group {interface | vlan vlanid { - vlanid}}

To delete a range of VLANs, use the following command:

no interface group vlan vlanid { - vlanid}

Parameters

- interface, interface,... Enter the keywords interface group and one of the interfaces — slot/port or VLAN number. Select the range of interfaces for bulk configuration. Spaces are not required between the commas. Comma-separated ranges can include VLANs and physical interfaces.

- Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10.

Slot/Port information need not contain a space before and after the dash. For example, both of the following commands are valid: interface group gigabitethernet 1/1 - 1/5; interface group gigabitethernet 1/1-1/5.

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

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
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.4(0.0) | Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.

Usage Information

The `interface group` command will create all the non-existent VLANs specified in the range. On successful command execution, the CLI switches to the interface group context.

The configuration commands inside the group context will be the similar to that of the existing range command.

Note: For release 9.4(0.0), the group command is supported only for VLANs and physical interfaces.

Example

```
Dell(conf)# interface group ?
gigabitethernet GigabitEthernet interface IEEE 802.3z
tengigabitethernet TenGigabit Ethernet interface
vlan VLAN keyword

Dell(conf)# interface group vlan 1 - 2 , tengigabitethernet 1/10
Dell(conf-if-group-vl-1-2,gi-1/10)# no shutdown
Dell(conf-if-group-vl-1-2,gi-1/10)# end
```

Related Commands

- `interface range` — configure a range of interfaces.
- `interface vlan` — configures a VLAN.

interface loopback

Configure a Loopback interface.

Syntax

```
interface loopback number
```

To remove a loopback interface, use the `no interface loopback number` command.

Parameters

- **number**
  
Enter a number as the interface number. The range is from 0 to 16383.

Defaults

Not configured.

Command Modes

- CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### interface managementEthernet

Configure the Management port on the system (either the Primary or Standby RPM).

**Syntax**

```
interface managementEthernet slot/port
```

**Parameters**

- `slot/port`:

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the S6100–ON.
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.
8.3.11.1 | Introduced on the S55, S60, and S4810.
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 1/1
Dell(conf-if-ma-1/1)#

Related Commands

- **management route** — configure a static route that points to the Management interface or a forwarding router.
- **speed (Management interface)** — Set the speed for the Management interface.

### interface null

Configure a Null interface on the switch.

**Syntax**

```
interface null number
```

**Parameters**

- **number**

  Enter zero (0) as the Null interface number.

**Defaults**

Not configured; number = 0

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

**Example**

```
Dell(conf)# interface null 0
Dell(conf-if-nu-0)#
```

**Related Commands**

- `interface` — configure a physical interface.
- `interface loopback` — configure a Loopback interface.
- `interface port-channel` — configure a port channel.
- `interface vlan` — configure a VLAN.
- `ip unreachables` — enable generation of internet control message protocol (ICMP) unreachable messages.

## interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

**Syntax**

```
interface range interface {slot/port | port} - {slot/port | port}, interface {slot/port | port} - {slot/port | port},...  
```

**Parameters**

- `interface {slot/port | port} - {slot/port | port}`: Enter `interface range` and one of the interfaces and then the interface information. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. The ranges can include VLANs, port-channels, and physical interfaces.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
  - For a Tunnel interface, enter the keyword `Tunnel` then a number from 1 to 16383.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.10(0.0) | Introduced on the S6100-ON.
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P2) | Introduced on the S4048-ON.
9.8(0.0P5) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4093 VLANs on E-Series. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

**Important Points to Remember:**

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

**Example (Bulk)**

```
Dell(conf)# interface range gigabitethernet 1/1 - 1/11, tengigabitethernet 3/3, gigabitethernet 3/10
% Warning: Non-existing ports (not configured) are ignored by interface-range
```

**Example (Multiple Ports)**

```
Dell(conf)# interface range gigabitethernet 2/10 - 2/23, gigabitethernet 2/12 - 2/17
Dell(conf-if-range-gi-2/10-2/23)#
```

**Example (Overlapping Ports)**

```
Dell(conf)# interface range gigabitethernet 2/3 - 2/11, gigabitethernet 2/3 - 2/23
Dell(conf-if-range-gi-2/3-2/23)#
```

**Usage Information**

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.
NOTE: If a range has VLAN, physical and port-channel interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN and port-channel only those respective interfaces should be configured in a particular range.

Example (Single Range)
This example shows a single range bulk configuration.

Dell(config)# interface range gigabitethernet 5/3 - 23
Dell(config-if-range-gi-5/3-5/23)# no shutdown
Dell(config-if-range-gi-5/3-5/23)#

Example (Multiple Range)
This example shows how to use commas to add different interface types to a range of interfaces.

Dell(config-if)# interface range gigabitethernet 5/1 - 5/23, gigabitethernet 1/1 - 1/2
Dell(config-if-range-gi-1/1-1/2,gi-5/1-5/23)# no shutdown
Dell(config-if-range-gi-1/1-1/2,gi-5/1-5/23)#

Example (Multiple Range)
This example shows how to use commas to add VLAN and port-channel interfaces to the range.

Dell(config-if)# interface range gigabitethernet 5/1 - 5/23, gigabitethernet 1/1 - 1/2,
Vlan 2-100, Port 1-25
Dell(config-if-range-gi-1/1-1/2,gi-5/1-5/23,vl-2-100,po-1-25)# no shutdown
Dell(config-if-range)#

Related Commands
- interface port-channel — configure a port channel group.
- interface vlan — configure a VLAN interface.
- show config (from INTERFACE RANGE mode) — display the bulk configuration interfaces.
- show range — display the bulk configuration ranges.
- interface range macro (define) — define a macro for an interface-range.

interface range macro (define)
Defines a macro for an interface range and then saves the macro in the running configuration.

Syntax
define interface range macro name interface , interface , ...

Parameters
name
Enter up to 16 characters for the macro name.

interface , interface...
Enter the keywords interface range and the interface information. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces.

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Tunnel interface, enter the keyword tunnel then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
None

Command Modes
CONFIGURATION
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4093 VLANs on E-Series. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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 gigabitethernet 1/1 - 1/3, gigabitethernet 5/1 - 5/22, gigabitethernet 3/1 - 3/8
Dell# show running-config | grep define
define interface-range test gigabitethernet 1/1 - 1/3, gigabitethernet 5/1 - 5/22, gigabitethernet 3/1 - 3/8
Dell(config)# interface range macro test
Dell(config-if-range-gi-1/1-1/3,te-5/1-5/22,te-3/1-3/8)#
```

### Related Commands

- `interface range` — configure a range of command (bulk configuration).
- `interface range macro name` — run 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

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example (Single Range)

This example shows the macro named test that was defined earlier.

```
Dell(config)# interface range macro test
Dell(config-if-range-gi-1/1-3,gi-5/1-47,gi-2/1-89)#
Dell
```

Related Commands

- `interface range` — configure a range of command (bulk configuration).
- `interface range macro (define)` — define a macro for an interface range (bulk configuration).

### interface vlan

Configure a VLAN. You can configure up to 4094 VLANs.

**Syntax**

```
interface vlan vlan-id [of-instance[of-id]]
```

**Parameters**

- `vlan-id`  
Enter a number as the VLAN Identifier. The range is from 1 to 4094.

- `of-instance[of-id]`  
Enter the keyword `of-instance` then the OpenFlow instance ID to add the VLAN to the specified OpenFlow instance. The range is from 1 to 8.

**Defaults**

Not configured, except for the Default VLAN, which is configured as VLAN 1.

**Command Modes**

CONFIGURATION

**NOTE:** Associate the OpenFlow instance with the VLAN when the VLAN is created. An existing VLAN cannot be associated with an OpenFlow instance.
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on the S4810; added support for OpenFlow.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

For more information about VLANs and the commands to configure them, see Virtual LAN (VLAN) Commands.

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC ACLs and IP ACLs are supported. For more information, see Access Control Lists (ACL).

The following features are not supported on VLANs associated with an OpenFlow instance:

- IPv4
- IPv6
- MTU

If OpenFlow VLANs are configured on the switch, spanning-tree protocols cannot be enabled simultaneously.

Example (Single Range)

Dell(conf)# int vlan 3
Dell(conf-if-vl-3)#

Related Commands

- interface — configure a physical interface.
- interface loopback — configure a loopback interface.
- interface null — configure a null interface.
- interface port-channel — configure a port channel group.
- show vlan — display the current VLAN configuration on the switch.
- shutdown — disable/enable the VLAN.
- tagged — add a Layer 2 interface to a VLAN as a tagged interface.
- untagged — add a Layer 2 interface to a VLAN as an untagged interface.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax

keepalive

To stop sending keepalive packets, use the no keepalive command.

Defaults

Enabled.
negotiation auto

Enable auto-negotiation on an interface.

Syntax

```
negotiation auto
```

To disable auto-negotiation, use the `no negotiation auto` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(2.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Version  Description
8.3.19.0  Introduced on the S4820T.
8.3.11.0  Introduced on the Z9000.
8.3.7.0  Introduced on the S4810.
8.1.1.0  Introduced on the E-Series.
7.6.1.0  Introduced on the S-Series.
7.5.1.0  Introduced on the C-Series.
pre-6.2.1.0  Introduced on the E-Series.

Usage Information
This command is supported on 10/100/1000 Base-T Ethernet interfaces.

You can use the command on the 10G ports on the device.

The no negotiation auto command is only available if you first manually set the speed of a port to 10Mbits or 100Mbits.

The negotiation auto command provides a mode option for configuring an individual port to forced-master/forced slave after you enable auto-negotiation.

NOTE: The mode option is not available on non-10/100/1000 Base-T Ethernet line cards.

If you do not use the mode option, the default setting is slave. If you do not configure forced-master or forced-slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

• Forced-master
• Force-slave
• Master
• Slave
• Auto-neg Error — typically indicates that both ends of the node are configured with forced-master or forced-slave.

CAUTION: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is, forced-master or forced-slave), the show interfaces command flaps between an auto-neg-error and forced-master/slave states.

You can display master/slave settings with the show interfaces command.

Example (Master/Slave)
Dell(conf)# interface gigabitethernet 1/1
Dell(conf-if)# neg auto
Dell(conf-if-autoneg)# ?
end Exit from configuration mode
exit Exit from autoneg configuration mode
mode Specify autoneg mode
no Negate a command or set its defaults
show Show autoneg configuration information
Dell(conf-if-autoneg)# mode ?
forced-master Force port to master mode
forced-slave Force port to slave mode
Dell(conf-if-autoneg)#

Example (Configured)
Dell# show interfaces configured
GigabitEthernet 1/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
   Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
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.

**monitor interface**

Monitor counters on a single interface or all interfaces. 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 the interface information:

  - For the Management interface on the stack-unit, enter the keyword `managementEthernet` then the slot/port information.
  - For a port channel interface, enter the keyword `port-channel` and then a number.
  - For a Tunnel interface, enter the keyword `tunnel` then the slot/port. The range is from 1 to 16383.
For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.

For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

In the Example, the delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>systest-3</td>
<td>Displays the host name assigned to the system.</td>
</tr>
<tr>
<td>monitor time</td>
<td>Displays the amount of time since the <code>monitor interface</code> command was entered.</td>
</tr>
<tr>
<td>time</td>
<td>Displays the amount of time the chassis is up (since last reboot).</td>
</tr>
<tr>
<td>m</td>
<td>Change the view from a single interface to all interfaces on the line card or visa-versa.</td>
</tr>
<tr>
<td>c</td>
<td>Refresh the view.</td>
</tr>
<tr>
<td>b</td>
<td>Change the counters displayed from Packets on the interface to Bytes.</td>
</tr>
<tr>
<td>r</td>
<td>Change the <code>[delta]</code> column from change in the number of packets/bytes in the last interval to rate per second.</td>
</tr>
<tr>
<td>l</td>
<td>Change the view to the next interface on the line card, or if in line card mode, the next line card in the chassis.</td>
</tr>
</tbody>
</table>
**Key**

a  
Change the view to the previous interface on the line card, or if in line card mode, the previous line card in the chassis.

T  
Increase the screen refresh rate.

t  
Decrease the screen refresh rate.

q  
Return to the CLI prompt.

---

### Example (Single Interface)

systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time: 03:26:26

Interface: gi 1/3, Enabled, Link is Up, Linespeed is 1000 Mbit

<table>
<thead>
<tr>
<th>Traffic statistics</th>
<th>Current Rate Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes:</td>
<td>9069828 43 Bps 86</td>
</tr>
<tr>
<td>Output bytes:</td>
<td>606915800 43 Bps 86</td>
</tr>
<tr>
<td>Input packets:</td>
<td>54001 0 pps 1</td>
</tr>
<tr>
<td>Output packets:</td>
<td>9401589 0 pps 1</td>
</tr>
<tr>
<td>64B packets:</td>
<td>67 0 pps 0</td>
</tr>
<tr>
<td>Over 64B packets:</td>
<td>49166 0 pps 1</td>
</tr>
<tr>
<td>Over 127B packets:</td>
<td>350 0 pps 0</td>
</tr>
<tr>
<td>Over 255B packets:</td>
<td>1351 0 pps 0</td>
</tr>
<tr>
<td>Over 511B packets:</td>
<td>286 0 pps 0</td>
</tr>
<tr>
<td>Over 1023B packets:</td>
<td>2781 0 pps 0</td>
</tr>
</tbody>
</table>

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

---

### Example (All Interfaces)

systest-3 Monitor time: 00:01:31 Refresh Intvl.: 2s Time: 03:54:14

Interface: Giants, Enabled, Link is Up, Linespeed is 1000 Mbit

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>In Packets [delta]</th>
<th>Out Packets [delta]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 1/1</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi 1/2</td>
<td>Up</td>
<td>61512</td>
<td>52</td>
</tr>
<tr>
<td>Gi 1/3</td>
<td>Up</td>
<td>63086</td>
<td>20</td>
</tr>
<tr>
<td>Gi 1/4</td>
<td>Up</td>
<td>14697471418</td>
<td>2661481</td>
</tr>
</tbody>
</table>

2661385

| Gi 1/5    | Up   | 3759               | 3 161959604         |
| Gi 1/6    | Up   | 4070               | 3 8680346           |
| Gi 1/7    | Up   | 61934              | 34 138734357        |
| Gi 1/8    | Up   | 61427              | 1 59960             |
| Gi 1/9    | Up   | 62039              | 53 104239232        |
| Gi 1/10   | Up   | 17740044091        | 372 7373849244      |
| Gi 1/11   | Up   | 18182889225        | 44 7184747584       |
| Gi 1/12   | Up   | 18182682056        | 0                  |
| Gi 1/13   | Up   | 14697471418        | 2661481             |
| Gi 1/14   | Up   | 61349              | 55 86281941         |
| Gi 1/15   | Up   | 59908              | 58 62060            |
| Gi 1/16   | Up   | 59909              | 1 61616             |
| Gi 1/17   | Up   | 0                  | 0 14950126          |
| Gi 1/18   | Up   | 0                  | 0                   |
| Gi 1/19   | Down | 0                  | 0                   |
| Gi 1/20   | Up   | 62134              | 54 62766            |
| Gi 1/21   | Up   | 60198              | 9 200899            |
| Gi 1/22   | Up   | 17304741100        | 3157554 10102508511 |

1114221
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 default is 1554.

Defaults

1554

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.5.1.0 Introduced on the C-Series.
pre-Version 6.2.1.0 Introduced on the E-Series.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (ip mtu command) must be enough bytes to include the Layer 2 header.

When you enter the no mtu command, Dell Networking OS reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU of 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.

<table>
<thead>
<tr>
<th>Layer 2 Overhead</th>
<th>Link MTU and IP MTU Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (untagged)</td>
<td>18 bytes</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>22 bytes</td>
</tr>
<tr>
<td>Untagged Packet with VLAN-Stack Header</td>
<td>22 bytes</td>
</tr>
<tr>
<td>Tagged Packet with VLAN-Stack Header</td>
<td>26 bytes</td>
</tr>
</tbody>
</table>

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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
### Version Description

- **8.3.11.1**  
  Introduced on the Z9000.
- **8.3.7.0**  
  Introduced on the S4810.
- **8.1.1.0**  
  Introduced on the E-Series.
- **7.6.1.0**  
  Introduced on the S-Series.
- **7.5.1.0**  
  Introduced on the C-Series.

### Usage Information

The following describes the `interface` command shown in the following example. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port now accepts:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the following example. This example shows output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- **True** — port is tagged
- **False** — port is untagged
- **Hybrid** — port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the following example. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.

> **NOTE:** Remove all other configurations on the port before you can remove the hybrid configuration from the port.

### Example

```bash
Dell(conf)# interface gigabitethernet 1/1  
Dell(conf-if-gi-1/1)# portmode hybrid  
Dell(conf-if-gi-1/1)# interface vlan 10  
Dell(conf-if-vl-10)# untagged gigabitethernet 1/1  
Dell(conf-if-vl-10)# interface vlan 20  
Dell(conf-if-vl-20)# tagged gigabitethernet 1/1  
Dell(conf-if-vl-20)#
```

### Example

```bash
Dell(conf-if-vl-20)# do show interfaces switchport  
Name: GigabitEthernet 1/1  
802.1QTagged: Hybrid  
Vlan membership:  
Vlan 10,  Vlan 20  
Native  VlanId: 10  
Dell(conf-if-vl-20)#
```

### Example (Vlan)

```bash
Dell(conf-if-vl-20)# interface vlan 10  
Dell(conf-if-vl-10)# no untagged gigabitethernet 1/1  
Dell(conf-if-vl-10)# interface vlan 20  
Dell(conf-if-vl-20)# no tagged gigabitethernet 1/1  
Dell(conf-if-vl-20)# interface gigabitethernet 1/1  
Dell(conf-if-vl-20)# no portmode hybrid  
Dell(conf-if-gi-1/1)#
```
rate-interval

Configure the traffic sampling interval on the selected interface.

Syntax
rate-interval seconds

Parameters
seconds
 Enter the number of seconds for which to collect traffic data. The range is from 5 to 299 seconds.

NOTE: Because polling occurs every 15 seconds, the number of seconds designated here rounds to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated, it rounds to 30; 45 to 59 seconds rounds to 45.

Defaults 299 seconds

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.1.1.0 Introduced

Usage Information The output of the show interfaces command displays the configured rate interval, along with the collected traffic data.

Related Commands  
  show interfaces — display information on physical and virtual interfaces.
**show config**

Display the interface configuration.

**Syntax**

```
show config
```

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.11.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
show config (from INTERFACE RANGE mode)
```

Display the bulk configured interfaces (interface range).

**Syntax**

```
show config
```

**Command Modes**

CONFIGURATION INTERFACE (conf-if-range)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
Dell(conf)# interface range gigabitethernet 1/1 - 1/2
Dell(conf-if-range-gi-1/1-2)# show config
!
interface GigabitEthernet 1/1
  no ip address
  switchport
  no shutdown
!
interface GigabitEthernet 1/2
  no ip address
  switchport
  no shutdown
Dell(conf-if-range-gi-1/1-2)#
```

**show interfaces**

Display information on a specific physical interface or virtual interface.

**Syntax**

```
show interfaces interface-type[-range]
```

**Parameters**

- `interface`
  
  Enter one of the following keywords and the interface information:
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For stack-units, enter the keywords `stack-unit` then the slot/port information.
  - For a Null interface, enter the keyword `null` then the Null interface number.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
  - For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.

**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.
-range

(Optional) Enter the range of interfaces for which you want to view the information. The format is interface-type slot/port-slot/port

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Added support for the tunnel interface type.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Updated Management Ethernet output to include two global IPv6 addresses on S4810 and Z9000 and added output example showing OpenFlow instance ID.</td>
</tr>
<tr>
<td>8.3.12.1</td>
<td>Updated command output to support multiple IPv6 addresses on S4810.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Output expanded to support eSR4 optics in Z9000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.2</td>
<td>Included SFP and SFP+ optics power detail in the E-Series and C-Series output.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4093 VLANs on the E-Series. Prior releases supported 2094.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Output expanded to include SFP+ media on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Changed the organization of the display output.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the Pluggable Media Type field in the E-Series output.</td>
</tr>
</tbody>
</table>

Usage Information

Use the show interfaces command for details on a specific interface.

- **NOTE:** In the CLI output, the power value is rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an snmp query returns the corresponding dbm value even though the CLI displays as 0.000.

- **NOTE:** After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there is no change in the line-rate.
The following table describes the `show interfaces` command shown in the 10G example.

<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet 1/1...</td>
<td>Interface type and administrative and line protocol status.</td>
</tr>
<tr>
<td>Hardware is...</td>
<td>Interface hardware information, assigned MAC address, and current address.</td>
</tr>
<tr>
<td>Pluggable media present...</td>
<td>Present pluggable media wavelength, type, and rate. The error scenarios are:</td>
</tr>
<tr>
<td></td>
<td>• Wavelength, Non-qualified — Dell ID is not present, but wavelength information is available from XFP or SFP serial data</td>
</tr>
<tr>
<td></td>
<td>• Wavelength, F10 unknown — Dell ID is present, but not able to determine the optics type</td>
</tr>
<tr>
<td></td>
<td>• Unknown, Non-qualified — if wavelength is reading error, and F10 ID is not present</td>
</tr>
<tr>
<td>Interface index...</td>
<td>Displays the interface index number the SNMP uses to identify the interface.</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.</td>
</tr>
<tr>
<td>MTU 1554...</td>
<td>Displays link and IP MTU information.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays the interface's line speed, duplex mode, and negotiation mode.</td>
</tr>
<tr>
<td>ARP type...</td>
<td>Displays the ARP type and the ARP timeout value for the interface.</td>
</tr>
<tr>
<td>Last clearing...</td>
<td>Displays the time when the <code>show interfaces</code> counters where cleared.</td>
</tr>
<tr>
<td>Queuing strategy...</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
<tr>
<td>Input Statistics:</td>
<td>Displays all the input statistics including:</td>
</tr>
<tr>
<td></td>
<td>• Number of packets and bytes into the interface</td>
</tr>
<tr>
<td></td>
<td>• Number of packets with VLAN tagged headers</td>
</tr>
<tr>
<td></td>
<td>• Packet size and the number of those packets inbound to the interface</td>
</tr>
<tr>
<td></td>
<td>• Number of Multicast and Broadcast packets:</td>
</tr>
<tr>
<td></td>
<td>• Multicasts = number of MAC multicast packets</td>
</tr>
<tr>
<td></td>
<td>• Broadcasts = number of MAC broadcast packets</td>
</tr>
<tr>
<td></td>
<td>• Number of runts, giants, and throttles packets:</td>
</tr>
<tr>
<td></td>
<td>• runts = number of packets that are less than 64B</td>
</tr>
<tr>
<td></td>
<td>• giants = packets that are greater than the MTU size</td>
</tr>
<tr>
<td></td>
<td>• throttles = packets containing PAUSE frames</td>
</tr>
<tr>
<td></td>
<td>• Number of CRC, overrun, and discarded packets:</td>
</tr>
<tr>
<td></td>
<td>• CRC = packets with CRC/FCS errors</td>
</tr>
<tr>
<td></td>
<td>• overrun = number of packets discarded due to FIFO overrun conditions</td>
</tr>
<tr>
<td></td>
<td>• discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing</td>
</tr>
<tr>
<td>Output Statistics:</td>
<td>Displays output statistics sent out of the interface including:</td>
</tr>
<tr>
<td></td>
<td>• Number of packets, bytes, and underruns out of the interface</td>
</tr>
<tr>
<td></td>
<td>• Packet size and the number of the packets outbound to the interface</td>
</tr>
</tbody>
</table>
### Line Description

- Number of Multicast, Broadcast, and Unicast packets:
  - Multicasts = number of MAC multicast packets
  - Broadcasts = number of MAC broadcast packets
  - Unicasts = number of MAC unicast packets

- Number of VLANs, throttles, discards, and collisions:
  - Vlans = number of VLAN tagged packets
  - throttles = packets containing PAUSE frames
  - discarded = number of packets discarded without any processing
  - collisions = number of packet collisions
  - wred=count both packets discarded in the MAC and in the hardware-based queues

### Rate information...
Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.

### Time since...
Elapsed time since the last interface status change (hh:mm:ss format).

### Example

```plaintext
Dell# show interfaces
TenGigabitEthernet 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:01:e8:8b:3d:e7
Current address is 00:01:e8:8b:3d:e7
Pluggable media present, Media type is unknown
Wavelength unknown
Interface index is 100992002
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d17h53m
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  0 packets, 0 bytes, 0 underruns
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts, 0 Unicasts
  0 throttles, 0 discarded, 0 collisions, 0 wredrops
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 3d17h51m
```

```plaintext
Dell# show interfaces
GigabitEthernet 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:01:e8:8b:3d:e7
Current address is 00:01:e8:8b:3d:e7
Pluggable media present, Media type is unknown
Wavelength unknown
Interface index is 100992002
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d17h53m
Queueing strategy: fifo
```
Input Statistics:
0 packets, 0 bytes
0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
0 Multicasts, 0 Broadcasts
0 runts, 0 giants, 0 throttles
0 CRC, 0 overrun, 0 discarded

Output Statistics:
0 packets, 0 bytes
0 Multicasts, 0 Broadcasts, 0 Unicasts
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 throttles, 0 discarded, 0 collisions, 0 wreddrops

Rate info (interval 299 seconds):
Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate

Time since last interface status change: 3d17h51m

Usage Information
The Management port is enabled by default (no shutdown). If necessary, use the ip address command to assign an IP address to the Management port. If two RPMs are installed in your system, use the show redundancy command to display which RPM is the Primary RPM.

Example
Dell# show interfaces gigabitethernet 1/1
GigabitEthernet 1/1 is up, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:41:77:95
  Current address is 00:01:e8:41:77:95
  Pluggable media present, SFP type is 1000BASE-SX
  Wavelength is 850nm
  Interface index is 100974648
  Port will not be disabled on partial SFM failure
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed 1000 Mbit
  Flowcontrol rx on tx on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interface" counters 1w0d5h
  Queueing strategy: fifo
  Input Statistics:
    0 packets, 0 bytes
    0 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 Vlans, 0 throttles, 0 discarded, 0 collisions, 0 wreddrops
  Rate info (interval 299 seconds):
    Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
    Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Time since last interface status change: 1w0d5h
Dell#

Example (Management Ethernet)
Dell# show interfaces managementethernet 1/1
ManagementEthernet 1/1 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:0b:a9:4c
  Current address is 00:01:e8:0b:a9:4c
  Pluggable media not present
  Interface index is 503595208
  Internet address is 10.11.201.5/16
  Link local IPv6 address: fe80::201:e8ff:fe0b:a94c/64
  Global IPv6 address: 2222::5/64
  Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10 Mbit, Mode full duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:01:08
Queueing strategy: fifo
  Input 943 packets, 78347 bytes, 190 multicast
  Received 0 errors, 0 discarded
  Output 459 packets, 102388 bytes, 15 multicast
  Output 0 errors, 0 invalid protocol
Time since last interface status change: 00:03:09

Example (Management Ethernet, two IPv6 addresses)

Dell# show interfaces managementethernet 1/1
ManagementEthernet 1/1 is up, line protocol is up
Hardware is DellForce10Eth, address is 00:01:e8:a0:bf:f3
Current address is 00:01:e8:a0:bf:f3
Pluggable media not present
Interface index is 302006472
Internet address is 10.16.130.5/16
Link local IPv6 address: fe80::201:e8ff:fea0:bff3/64
Global IPv6 address: 1::1/
Global IPv6 address: 2::1/64
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:06:14
Queueing strategy: fifo
Input 791 packets, 62913 bytes, 775 multicast
Received 0 errors, 0 discarded
Output 21 packets, 3300 bytes, 20 multicast
Output 0 errors, 0 invalid protocol
Time since last interface status change: 00:06:03

Example (OpenFlow instance)

Dell# show interfaces vlan 6
Vlan 6 is down, line protocol is down
Address is 00:01:e8:8a:e1:8c, Current address is 00:01:e8:8a:e1:8c
Interface index is 1107525638
of-instance: 2
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:05:12
Queueing strategy: fifo
Time since last interface status change: 00:05:12

Related Commands

- show interfaces configured – display any interface with a non-default configuration.
- show inventory (S-Series and Z-Series) – display the S-Series and Z-Series switch types, components (including media), Dell Networking OS version including hardware identification numbers, and configured protocols.
- show ip interface – display Layer 3 information about the interfaces.
- show range – display all interfaces configured using the interface range command.

show interfaces configured

Display any interface with a non-default configuration.

Syntax

    show interfaces configured

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### Version Description

8.1.1.0  Introduced on the E-Series.
7.6.1.0  Introduced on the S-Series.
7.5.1.0  Introduced on the C-Series.
6.4.1.0  Changed the organization of the display output.

---

**Example**

```plaintext
Dell# show interfaces configured
GigabitEthernet 1/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
  10 packets, 10000 bytes
  0 Vlans
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 10 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 runts, 0 giants, 0 throttles
  0 CRC, 0 overrun, 0 discarded
Output Statistics:
  1 packets, 64 bytes, 0 underruns
  1 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 1 Broadcasts, 0 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
  Input 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
  Output 00.00 Mbits/sec, 0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:04:59
Dell#
```

---

**Related Commands**

- `show interfaces` — display information on a specific physical interface or virtual interface.

---

### show interfaces dampening

Display interface dampening information.

**Syntax**

```
show interfaces dampening [[interface] [summary] [detail]]
```

**Parameters**

- `interface`  
  (Optional) Enter one of the following keywords and the interface information:
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**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 - 1/1/4`.

### summary
(Optional) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.

### detail
(Optional) Enter the keyword `detail` to display detailed interface dampening data.

**Defaults**
None

**Command Modes**
EXEC

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**
```
Dell# show interfaces dampening
Interface Supp  Flaps Penalty Half-Life Reuse Suppress Max-Sup
   State
Gi 1/2   Up  0   0  20  800   4500  120
Gi 1/10  Up  0   0   5  750   2500  20
Dell#
```

**Related Commands**
- `dampening` — configure dampening on an interface.
- `show interfaces` — display information on a specific physical interface or virtual interface.
show interfaces configured — display any interface with a non-default configuration.

show interfaces phy

Display auto-negotiation and link partner information.

Syntax

show interfaces gigabitethernet slot/port phy

Parameters

- gigabitethernet
  - Enter the keyword gigabitethernet then the slot/port information.

- tengigabitethernet
  - Enter the keyword tengigabitethernet then the slot or port information.

- 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 - 1/1/4.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>6.5(4.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show interfaces gigabitethernet command following example.

Mode Control
- Indicates if auto negotiation is enabled. If so, indicates the selected speed and duplex.
| **Mode Status** | Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the autoNegComplete field and the linkstatus field read “True.” |
| **AutoNegotiation Advertise** | Displays the control words the local interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the local interface supports. |
| **AutoNegotiation Remote Partner’s Ability** | Displays the control words the remote interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the remote interface supports. |
| **AutoNegotiation Expansion** | ParallelDetectionFault is the handshaking scheme in which the link partner continuously transmit an “idle” data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner or else no link can be established. |
| **1000Base-T Control** | 1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting a speed to 1000 Mbps with the speed command without auto-negotiation. E-Series line cards support both full-duplex and half-duplex 1000BaseT. |
| **Phy Specific Control** | Values are: |
| | • 0 - Manual MDI |
| | • 1 - Manual MDIX |
| | • 2 - N/A |
| | • 3 - Auto MDI/MDIX |
| **Phy Specific Status** | Displays PHY-specific status information. Cable length represents a rough estimate in meters: |
| | • 0 - < 50 meters |
| | • 1 - 50 - 80 meters |
| | • 2 - 80 - 110 meters |
| | • 3 - 110 - 140 meters |
| | • 4 - 140 meters |
| **Link Status: Up or Down** | |
| **Speed:** | |
| | • Auto |
| | • 1000MB |
| | • 100MB |
| | • 10MB |

**Example**

```
Dell# show interfaces gigabitethernet 1/1 phy
Mode Control:
 SpeedSelection: 10b
 AutoNeg: ON
 Loopback: False
 PowerDown: False
 Isolate: False
 DuplexMode: Full
 Mode Status:
 AutoNegComplete: False
 RemoteFault: False
 LinkStatus: False
 JabberDetect: False
 AutoNegotation Advertise:
```
show interfaces stack-unit

Display information on all interfaces on a specific S-Series or Z-Series stack member.

Syntax

show interfaces stack-unit unit-number

Parameters

unit-number Enter the stack member number.

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.
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.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.

Example

Dell# show interfaces stack-unit 1
GigabitEthernet 1/1 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:4c:f2:82
Current address is 00:01:e8:4c:f2:82
Pluggable media not present
Interface index is 34129154

Related Commands

• show interfaces — display information on a specific physical interface or virtual interface.
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto, Mode auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3w0d17h
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  5144 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
  0 Multicasts, 0 Broadcasts
  0 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: 3w0d17h
GigabitEthernet 1/2 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:4c:f2:83
  Current address is 00:01:e8:4c:f2:83
!------------------output truncated -----------------!

Related Commands
• show hardware stack-unit — display data plane and management plane input/output statistics.
• show interfaces — display information on a specific physical interface or virtual interface.

show interfaces status

To display status information on a specific interface only, display a summary of interface information or specify a stack-unit slot and interface.

Syntax
show interfaces [interface | stack-unit slot-number] status

Parameters

interface

(OPTIONAL) Enter one of the following keywords the interface information:

• For a port channel interface, enter the keywords port-channel then a number.
• For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

(1) 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 – 1/1/4.
stack-unit slot-number

(Optional) Enter the keyword stack-unit then the slot number. The range is from 0 to 5.

Defaults
None

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show interfaces status
Port    Description  Status  Speed   Duplex  Vlan
Gi 1/1  Up           1000 Mbit Auto --
Gi 1/2  Down         Auto     Auto   1
Gi 1/3  Down         Auto     Auto   1
Gi 1/4  Down         Auto     Auto   --
Gi 1/5  DellPort     Up       1000 Mbit Auto  30-130
Gi 1/6  Down         Auto     Auto   --
Gi 1/7  Down         Auto     Auto   --
Gi 1/8  Up           1000 Mbit Auto 1502,1504,1506-1508,1602
Gi 1/9  Down         Auto     Auto   --
Gi 1/10 Down         Auto     Auto   --
Gi 1/11 Down         Auto     Auto   --
Gi 1/12 Down         Auto     Auto   --
Gi 1/13 Down         Auto     Auto   --
Gi 1/14 Down         Auto     Auto   --
Gi 1/15 Down         Auto     Auto   --
Gi 1/16 Down         Auto     Auto   --
Dell#
```

Related Commands
- show interfaces — display information on a specific physical interface or virtual interface.
show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces’ IEEE 802.1Q tag status and VLAN membership.

Syntax

show interfaces switchport [interface-type | stack-unit unit-id ]

Parameters

interface-type  (OPTIONAL) Enter one of the following keywords and the interface information:

- For a port channel interface, enter the keywords port-channel then a number.
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a backup interface for this interface, enter the keyword backup.

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 then the stack member number.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
</tbody>
</table>
### Version Description
- **8.2.1.0**: Added support for 4093 VLANs on E-Series.
- **8.1.1.0**: Introduced on the E-Series.
- **7.6.1.0**: Support added for hybrid port/native VLAN, introduced on the S-Series.
- **7.5.1.0**: Introduced on the C-Series.

#### E-Series legacy command

### Usage Information
The following describes the `show interfaces switchport` command for the following example.

<table>
<thead>
<tr>
<th>Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the interface's type, slot/port number.</td>
</tr>
<tr>
<td>802.1QTagged</td>
<td>Displays whether the VLAN tagged (&quot;True&quot;), untagged (&quot;False&quot;), or hybrid (&quot;Hybrid&quot;), which supports both untagged and tagged VLANs by the port.</td>
</tr>
<tr>
<td>Vlan membership</td>
<td>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 the port.</td>
</tr>
</tbody>
</table>

#### Example
```
Dell# show interfaces switchport
Name: GigabitEthernet 1/1
  802.1QTagged: Hybrid
  Vlan membership:
  Vlan 2, Vlan 20
  Native VlanId: 20

Name: GigabitEthernet 1/2
  802.1QTagged: True
  Vlan membership:
  Vlan 2

Name: GigabitEthernet 1/3
  802.1QTagged: True
  Vlan membership:
  Vlan 2

Name: GigabitEthernet 1/4
  802.1QTagged: True
  Vlan membership:
  Vlan 2
--More--
```

#### Related Commands
- `interface` — configure a physical interface on the switch.
- `show ip interface` — display Layer 3 information about the interfaces.
- `show interfaces` — display information on a specific physical interface or virtual interface.
- `show interfaces transceiver` — display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

### show interfaces transceiver
Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

#### Syntax
```
show interfaces interfaces transceiver
```
(OPTIONAL) Enter one of the following keywords and then the interface information:

- For a port channel interface, enter the keywords port-channel and then a number.
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet and then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet and 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 - 1/1/4.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.11.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Output augmented with diagnostic data for pluggable media.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Removed three fields in the output: Vendor Name, Vendor OUI, and Vendor PN.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>6.5.4.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show interfaces transceiver` command shown in the following example.
<table>
<thead>
<tr>
<th>Line</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Power measurement type</td>
<td>Output depends on the vendor, typically either “Average” or “OMA” (Receiver optical modulation amplitude).</td>
</tr>
<tr>
<td>Temp High Alarm threshold</td>
<td>Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.</td>
</tr>
<tr>
<td>Voltage High Alarm threshold</td>
<td>Displays the interface index number used by SNMP to identify the interface.</td>
</tr>
<tr>
<td>Bias High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power Low Alarm threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>RX Power High Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temp Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Voltage Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Bias Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>TX Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Power Low Warning threshold</td>
<td>Factory-defined setting. Value can differ between SFP and SFP+.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Line</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voltage</td>
<td>Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/warning flag is set to true.</td>
</tr>
<tr>
<td>Tx Bias Current</td>
<td>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.</td>
</tr>
<tr>
<td>Tx Power</td>
<td>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.</td>
</tr>
<tr>
<td>Rx Power</td>
<td>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.</td>
</tr>
<tr>
<td>Data Ready state Bar</td>
<td>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.</td>
</tr>
<tr>
<td>Rx LOS state</td>
<td>This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.</td>
</tr>
<tr>
<td>Tx Fault state</td>
<td>This is the digital state of the Tx Fault output pin.</td>
</tr>
<tr>
<td>Rate Select state</td>
<td>This is the digital state of the SFP rate_select input pin.</td>
</tr>
<tr>
<td>RS state</td>
<td>This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.</td>
</tr>
<tr>
<td>Tx Disable state</td>
<td>If the admin status of the port is down then this flag is set to true.</td>
</tr>
<tr>
<td>Temperature High Alarm Flag</td>
<td>This can be either true or false, depending on the Current temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage High Alarm Flag</td>
<td>This can be either true or false, depending on the Current voltage value displayed above.</td>
</tr>
<tr>
<td>Tx Bias High Alarm Flag</td>
<td>This can be either true or false, depending on the present Tx bias current value displayed above.</td>
</tr>
<tr>
<td>Tx Power High Alarm Flag</td>
<td>This can be either true or false, depending on the Current Tx bias power value displayed above.</td>
</tr>
<tr>
<td>Rx Power High Alarm Flag</td>
<td>This can be either true or false, depending on the Current Rx power value displayed above.</td>
</tr>
<tr>
<td>Temperature Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current temperature value displayed above.</td>
</tr>
<tr>
<td>Voltage Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current voltage value displayed above.</td>
</tr>
<tr>
<td>Tx Bias Low Alarm Flag</td>
<td>This can be either true or false, depending on the Tx bias current value displayed above.</td>
</tr>
<tr>
<td>Tx Power Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current Tx power value displayed above.</td>
</tr>
<tr>
<td>Rx Power Low Alarm Flag</td>
<td>This can be either true or false, depending on the Current Rx power value displayed above.</td>
</tr>
<tr>
<td>Temperature High Warning Flag</td>
<td>This can be either true or false, depending on the Current temperature value displayed above.</td>
</tr>
</tbody>
</table>
### Line Description

**Voltage High Warning Flag**
- This can be either true or false, depending on the Current Voltage value displayed above.

**Tx Bias High Warning Flag**
- This can be either true or false, depending on the Tx bias current value displayed above.

**Tx Power High Warning Flag**
- This can be either true or false, depending on the Current Tx power value displayed above.

**Rx Power High Warning Flag**
- This can be either true or false, depending on the Current Rx power value displayed above.

**Temperature Low Warning Flag**
- This can be either true or false, depending on the Current Temperature value displayed above.

**Voltage Low Warning Flag**
- This can be either true or false, depending on the Current Voltage value displayed above.

**Tx Bias Low Warning Flag**
- This can be either true or false, depending on the present Tx bias current value displayed above.

**Tx Power Low Warning Flag**
- This can be either true or false, depending on the Current Tx power value displayed above.

**Rx Power Low Warning Flag**
- This can be either true or false, depending on the Current Rx power value displayed above.

### Example

Dell# show interfaces GigabitEthernet 1/1 transceiver
SFP is present.

**SFP 0 Serial Base ID fields**
- **Id** = 0x03
- **Ext Id** = 0x04
- **Connector** = 0x07
- **Transceiver Code** = 0x00 0x00 0x01 0x20 0x40 0x0c 0x05
- **Encoding** = 0x01
- **BR Nominal** = 0x15
- **Length (9um) Km** = 0x00
- **Length (9um) 100m** = 0x00
- **Length (50um) 10m** = 0x00
- **Length (62.5um) 10m** = 0x00
- **Length (Copper) 10m** = 0x00
- **Vendor Rev** = A
- **Laser Wavelength** = 850 nm
- **CheckCodeBase** = 0x66
- **Serial Extended ID fields**
- **Options** = 0x00 0x12
- **BR max= 0**
- **BR min= 0**
- **Vendor SN= P5N1ACE**
- **Datecode** = 040528
- **CheckCodeExt** = 0x5b

**SFP 1 Diagnostic Information**

**Rx Power measurement type** = Average

**Temp High Alarm threshold** = 95.000C
- **Voltage High Alarm threshold** = 3.900V
- **Bias High Alarm threshold** = 17.000mA
- **TX Power High Alarm threshold** = 0.631mW
- **RX Power High Alarm threshold** = 1.259mW
- **Temp Low Alarm threshold** = -25.000C
- **Voltage Low Alarm threshold** = 2.700V
- **Bias Low Alarm threshold** = 1.000mA
- **TX Power Low Alarm threshold** = 0.067mW
SFP 1 RX Power Low Alarm threshold = 0.010mW
===================================
SFP 1 Temp High Warning threshold = 90.000°C
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 = -20.000°C
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 = 39.930°C
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 — configure a physical interface on the switch.
• show ip interface — display Layer 3 information about the interfaces.
• show interfaces — display information on a specific physical interface or virtual interface.
• show inventory (S-Series and Z-Series) — display the switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.

show interfaces vlan

Display VLAN statistics.

Syntax
show interfaces vlan {vlan-id} [LINE] [description]

Parameters
• vlan-id
  Enter the interface VLAN number. The range is from 1 to 4094.
• LINE
  (OPTIONAL) Enter the name of the VLAN.
• description
  Displays the VLAN interface information with description.

Command Modes
• EXEC
• EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

## Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

## Usage Information

**NOTE:** This command also enables you to view information corresponding to a range of ports.

- 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 interface-type 1 - 4`.

### Example

```
Dell# show interfaces vlan 10
Vlan 10 is up, line protocol is down
Address is 90:b1:1c:f4:99:ce, Current address is 90:b1:1c:f4:99:ce
Interface index is 1107787786
Internet address is not set
Mode of IPv4 Address Assignment: NONE
DHCP Client-ID: 90b11cf499ce
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 2d17h26m
Queueing strategy: fifo
Time since last interface status change: 2d17h26m
Input Statistics:
0 packets, 0 bytes
Output Statistics:
0 packets, 0 bytes, 0 underruns
```

## Related Commands

- `show interfaces` — display information on a specific physical interface or virtual interface.

## show range

Display all interfaces configured using the `interface range` command.

### Syntax

```
show range
```

### Command Modes

- INTERFACE RANGE (config-if-range)

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4093 VLANs on E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Example**

Dell(conf-if-range-gi-2/2,fo-2/56)# show range
2/2 - 0
2/56 - 0
Dell(conf-if-range-gi-2/2,fo-2/56)#

**Related Commands**
- `interface` — configure a physical interface on the switch.
- `show ip interface` — display Layer 3 information about the interfaces.
- `show interfaces` — display information on a specific physical interface or virtual interface.

### show running-config ecmp-group

Display interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution using the `ecmp-group` monitoring enable command. The ECMP group could have a LAG or a list of 10G/40 interfaces (not just LAG link-bundles).

**Syntax**

```
show running-config ecmp-group
```

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version Description
8.3.10.0 Introduced on the S4810.

Related Commands
- `ecmp-group` — configure a mechanism to monitor traffic distribution.

**shutdown**

Disable an interface.

**Syntax**
```
shutdown
```

To activate an interface, use the `no shutdown` command.

**Defaults**
The interface is disabled.

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Usage Information**
The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, enter `no shutdown` on the port channel interface and at least one interface within that port channel.

The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.
speed (for 10/100/1000/10000 interfaces)

Set the speed for 10/100/1000/10000 interfaces. Set both sides of a link to the same speed (10/100/1000/10000) or to auto or the link may not come up.

Syntax

```
speed {10 | 100 | 1000 | 10000 | auto}
```

To return to the default setting, use the `no speed {10 | 100 | 1000 | 10000}` command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enter the keyword 10 to set the interface's speed to 10 Mb/s.</td>
</tr>
</tbody>
</table>

**NOTE:** This interface speed is not supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card. If the command is entered for these interfaces, an error message appears.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Enter the keyword 100 to set the interface's speed to 10/100 Mb/s.</td>
</tr>
</tbody>
</table>

**NOTE:** When this setting is enabled, only 100Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Enter the keyword 1000 to set the interface's speed to 1000 Mb/s. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code>.</td>
</tr>
</tbody>
</table>

**NOTE:** When this setting is enabled, only 1000Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>Enter the keyword 10000 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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enter the keyword auto to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to <code>negotiation auto</code>.</td>
</tr>
</tbody>
</table>

Defaults auto

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Added support for fanned–out 1 Gigabit SFP port.</td>
</tr>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.3.1.0 | Supported on LC-EH-GE-50P or the LC-EJ-GE-50P cards.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.

**E-Series legacy command**

**Usage Information**

This command is found on the 10/100/1000/10000 Base-T Ethernet interfaces.

When you enable `auto`, the system performs an automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 10/100/1000/10000 interface, confirm the negotiation `auto` command setting. Both sides of the link must have auto-negotiation either enabled or disabled. For speed settings of 1000 or `auto`, the software sets the link to auto-negotiation and you cannot change that setting.

**NOTE:** Starting with Dell Networking OS version 7.8.1.0, when you use a copper SFP2 module with catalog number GP-SFP2-1T in the S25P model of the S-Series, you can manually set its speed with the `speed` command. When you set the speed to 10 or 100 Mbps, you can also use the `duplex` command.

If you use an active optical cable (AOC), you can convert the QSFP+ port to a 10 Gigabit SFP+ port or 1 Gigabit SFP port. Use the `speed` command to enable the required speed.

**Related Commands**

- `duplex (10/100 Interfaces)` — configures duplex mode on physical interfaces.
- `negotiation auto` — enable or disable auto-negotiation on an interface.

### speed (Management interface)

Set the speed for the Management interface.

**Syntax**

```
speed {10 | 100 | 1000 | auto}
```

To return to the default setting, use the `no speed` command.

**Parameters**

- **10**
  - Enter the keyword `10` to set the interface's speed to 10 Mb/s.
- **100**
  - Enter the keyword `100` to set the interface's speed to 100 Mb/s.
- **1000**
  - Enter the keyword `1000` to set the interface's speed to 1000 Mb/s.
- **auto**
  - Enter the keyword `auto` to set the interface to auto-negotiate its speed.

**Defaults**

`auto`

**Command Modes**

`INTERFACE`
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the S55, S60, and S4810</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

This command is found on the Management interface only.

Related Commands

- `interface ManagementEthernet` — configure the Management port on the system (either the Primary or Standby RPM).
- `duplex (10/100 Interfaces)` — configure duplex mode on physical interfaces with the speed set to 10/100.
- `management route` — configure a static route that points to the Management interface or a forwarding router.

```
switchport
```

Place an interface in Layer 2 mode.

**Syntax**

`switchport [[backup interface {interface | port-channel number}] | mode private-vlan {host | promiscuous | trunk}]`

To remove an interface from Layer 2 mode and place it in Layer 3 mode, enter the `no switchport` command. If a switchport backup interface is configured, first remove the backup configuration. To remove a switchport backup interface, enter the `no switchport backup interface` command.

**Parameters**

- `backup`
  - (OPTIONAL) Use this option to configure a redundant Layer 2 link without using Spanning Tree. The keyword `backup` configures a backup port so that if the primary port fails, the backup port changes to the up state. If the primary later comes up, it becomes the backup.

- `interface interface`
  - (OPTIONAL) Enter any of the following keywords and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

---

**Related Commands**

- `interface ManagementEthernet` — configure the Management port on the system (either the Primary or Standby RPM).
- `duplex (10/100 Interfaces)` — configure duplex mode on physical interfaces with the speed set to 10/100.
- `management route` — configure a static route that points to the Management interface or a forwarding router.
(OPTIONAL) Enter the keywords port-channel if the backup port is a static or dynamic port channel.

mode

(Optional) Enter the keyword mode to set the interface mode.

private-vlan

(Optional) Enter the keywords private-vlan to set the interface mode to private VLAN mode.

host

(Optional) Enter the keyword host to set the private VLAN interface to host mode.

promiscuous

(Optional) Enter the keyword promiscuous to set the private VLAN interface to promiscuous mode.

trunk

(Optional) Enter the keyword trunk to set the private VLAN interface to trunk mode.

Defaults

Disabled — interface is in Layer 3 mode.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for port-channel interfaces (the port-channel number option).</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the backup interface option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If an IP address or VRRP group is assigned to the interface, you cannot use the switchport command on the interface. To use the switchport command on an interface, only the no ip address and no shutdown statements must be listed in the show config output.

When you enter the switchport command, the interface is automatically added to the default VLAN.
To use the `switchport backup interface` command on a port, first enter the `switchport` command. For more information, see “Configuring Redundant Links” in the Layer 2 section in the Dell Networking OS Configuration Guide.

### 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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Usage Information**

The wavelength can be configured only on a tunable 10-Gigabit SFP+ optic. The wavelength range is from 1528.3 nm to 1568.77 nm.

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:

```
Dell(conf-if-gi-1/1)# wavelength 1528.30
```

**Related Commands**

- `show config` — displays the interface configuration.

### Egress Interface Selection (EIS) Commands

The following commands are Egress Interface Selection (EIS) commands.

**application**

Configure the management egress interface selection.

**Syntax**

```
application (all | application-type)
```

To remove a management application configuration, use the `no application (all | application-type)` command.
Parameters | application-type | Enter any of the following keywords:
| | • For DNS, enter the keyword dns.
| | • For FTP, enter the keyword ftp.
| | • For NTP, enter the keyword ntp.
| | • For Radius, enter the keyword radius.
| | • For sFlow collectors, enter the keyword sflow-collector.
| | • For SNMP (traps and MIB responses), enter the keywords snmp.
| | • For SSH, enter the keyword ssh.
| | • For Syslog, enter the keyword syslog.
| | • For TACACS, enter the keyword tacacs.
| | • For Telnet, enter the keyword telnet.
| | • For TFTP, enter the keyword tftp.

all
Configure all applications.

Defaults
None.

Command Modes
EIS Mode (conf-mgmt-eis)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

**application (for HTTP and ICMP)**

Configure the management egress interface selection for HTTP and ICMP.

**NOTE:** Only the options that have been newly introduced are described here. For a complete description on all of the keywords and variables that are available with this command, refer the respective Command Reference Guide of the applicable platform of the Release 9.2(0.0) documentation set.

Syntax

```
application {all | application-type}
```

To remove a management application configuration, use the no application {all | application-type} command.

Parameters

<table>
<thead>
<tr>
<th>application-type</th>
<th>Enter any of the following keywords:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For HTTP, enter the keyword http.</td>
</tr>
<tr>
<td></td>
<td>• For ICMP, enter the keyword icmp.</td>
</tr>
</tbody>
</table>
Configure all applications.

Defaults

Command Modes

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3.(0.0)</td>
<td>Added support for the HTTP and ICMP traffic on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

Clear management application packet counters for all management application types.

Syntax

`clear management application pkt-cntr`

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

Clear management application packet fallback counters for all management application types.

Syntax

`clear management application pkt-fallback-cntr`

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
management egress-interface-selection

To make configured application traffic egress through the management port instead of the front-end (FE) port, enable and configure a management egress interface.

Syntax

management egress-interface-selection

To disable and remove management egress interface selection (EIS) configurations, use the no management egress-interface-selection command.

Defaults

None.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

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.
9.2(0.2) Introduced on the Z9000, S4810, and S4820T.

show ip management-eis-route

Display the management routes used by EIS.

Syntax

show ip management-eis-route

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

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.
9.2(0.2) Introduced on the Z9000, S4810, and S4820T.

Example

Dell# show ip management-eis-route
Destination    Gateway                 State      Route Source
--------------- -------                 -----      ------------
10.11.0.0/16    ManagementEthernet 1/1 Connected Connected
172.16.1.0/24   10.11.192.4             Active     Static
show management application pkt-cntr

Display the number of packets for each application type that have taken the management route.

Syntax
show management application pkt-cntr

Defaults
None.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

Example

Dell# show management application pkt-cntr

dns : 2
ftp : 0
ntp : 0
radius : 0
sflow-collector : 0
snmp : 0
ssh : 0
syslog : 0
tacacs : 0
telnet : 0
tftp : 0

show management application pkt-fallback-cntr

Display the number of packets for each application type that have been rerouted to the default routing table due to management port or route lookup failure.

Syntax
show management application pkt-fallback-cntr

Defaults
None.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>
## 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.

- The platform supports 128 port channels and 16 members per port channel.

As 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. But stack members can provide those ports.

**NOTE:** The Dell Networking OS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about Dell Networking OS link aggregation control protocol (LACP) for dynamic LAGs, refer to the Link Aggregation Control Protocol (LACP) chapter. For more information about configuring and using Port Channels, refer to the *Dell Networking OS Configuration Guide*.

### channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

**Syntax**

```
channel-member interface
```

To delete an interface from a Port Channel, use the `no channel-member interface` command.

**Parameters**

- **interface**
  
  (OPTIONAL) Enter any of the following keywords and the interface information:
  
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults**

Not configured.

**Command Modes**

INTERFACE PORTCHANNEL

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
### Version Description
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.2(1.0)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.5.1.0** Added support for 4-port 40G line cards on the E-Series.
- **8.3.7.0** Introduced on the S4810.
- **8.1.1.0** Introduced on the E-Series.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.
- **pre-Version 6.2.1.0** Introduced on the E-Series.

### Usage Information
Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the `shutdown`, `description`, `mtu`, and `ip mtu` commands can be configured on an interface if it is added to a Port Channel. The `mtu` and `ip mtu` commands are only available when the chassis is in Jumbo mode.

Link MTU and IP MTU considerations for Port Channels are:
- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

You can have 16 interfaces per Port Channel. 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).

For more information about Port Channels, refer to the Dell Networking OS Configuration Guide.

### Related Commands
- `description` — assign a descriptive text string to the interface.
- `interface port-channel` — create a Port Channel interface.
- `shutdown` — disable/enable the port channel.
Group two LAGs in a supergroup ("fate-sharing group" or "failover group").

Syntax

```plaintext
group group_number port-channel number port-channel number
```

To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters

- **group_number**: Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
- **port-channel number**: Enter the keywords `port-channel` then an existing LAG number. Enter this keyword/variable combination twice, identifying the two paired LAGs.

Defaults

None

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series, E-Series, and S-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `port-channel failover-group` — access PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.
- `show interfaces port-channel` — display information on configured Port Channel groups.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing 16 physical interfaces on the S-Series.

Syntax

```plaintext
interface port-channel channel-number
```

Interface
To delete a Port Channel, use the `no interface port-channel channel-number` command.

**Parameters**

`channel-number` For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

The `shutdown`, `description`, and `name` commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can only have the `shutdown`, `description`, and `name` commands configured. The Port Channel's configuration is applied to the interfaces within the Port Channel.

A Port Channel can contain any physical interface. Based on the first interface configured in the Port Channel and enabled, Dell Networking OS determines the common speed. For more information, refer to `channel-member`.

If the line card is in a Jumbo mode chassis, you can also configure the `mtu` and `ip mtu` commands. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

**NOTE:** In a Jumbo-enabled system, all members of a Port Channel must be configured with the same link MTU values and the same IP MTU values.

**Example**

```
Dell(conf)# int port-channel 2
Dell(conf-if-po-2)#
```
Related Commands

- channel-member — add a physical interface to the LAG.
- interface — configure a physical interface.
- interface loopback — configure a Loopback interface.
- interface null — configure a null interface.
- interface vlan — configure a VLAN.
- shutdown — disable/enable the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in “oper up” status for the LAG to be also in “oper up” status.

Syntax

minimum-links number

Parameters

number Enter the number of links in a LAG that must be in “oper up” status. The range is from 1 to 16. The default is 1.

Defaults

1

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-Version 6.2.1.0 Introduced on the E-Series.

Usage Information

If you use this command to configure the minimum number of links in a LAG that must be in “oper up” status, the LAG must have at least that number of “oper up” links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.
port-channel failover-group

To configure a LAG failover group, access PORT-CHANNEL FAILOVER-GROUP mode.

Syntax

port-channel failover-group

To remove all LAG failover groups, use the no port-channel failover-group command.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.

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, see the “Port Channel” section in the Dell Networking OS Configuration Guide.

Related Command

• group — group two LAGs in a supergroup (“fate-sharing group”).
• show interfaces port-channel — display information on configured Port Channel groups.

show config

Display the current configuration of the selected LAG.

Syntax

show config

Command Modes

INTERFACE PORTCHANNEL
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-Version 6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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 then a number. The range is from 1 to 128.

brief (OPTIONAL) Enter the keyword brief to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

description (OPTIONAL) Displays the port-channel information with description.

Command Modes
- EXEC
- EXEC Privilege
### Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Added support to display the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series. Modified to display the LAG failover group status.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### E-Series legacy command

### Usage Information

The following describes the `show interfaces port-channel` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Channel</td>
<td>Displays the LAG’s status. In the Example, the status of the LAG’s LAG fate-sharing group (“Failover-group”) is listed.</td>
</tr>
<tr>
<td>Hardware is...</td>
<td>Displays the interface’s hardware information and its assigned MAC address.</td>
</tr>
<tr>
<td>Port-channel is</td>
<td>Indicates whether the LAG is part of a LAG fate-sharing group (“Failover-group”).</td>
</tr>
<tr>
<td>part...</td>
<td></td>
</tr>
<tr>
<td>Internet address..</td>
<td>States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.</td>
</tr>
<tr>
<td>MTU 1554...</td>
<td>Displays link and IP MTU.</td>
</tr>
<tr>
<td>LineSpeed</td>
<td>Displays the interface’s line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.</td>
</tr>
<tr>
<td>Members in this...</td>
<td>Displays the interfaces belonging to this port channel.</td>
</tr>
<tr>
<td>ARP type:...</td>
<td>Displays the ARP type and the ARP timeout value for the interface.</td>
</tr>
<tr>
<td>Last clearing...</td>
<td>Displays the time when the <code>show interfaces</code> counters were cleared.</td>
</tr>
<tr>
<td>Queuing strategy,</td>
<td>States the packet queuing strategy. FIFO means first in first out.</td>
</tr>
<tr>
<td>packets input...</td>
<td>Displays the number of packets and bytes into the interface.</td>
</tr>
<tr>
<td>Input 0 IP packets</td>
<td>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.</td>
</tr>
</tbody>
</table>
Field Description

0 64-byte... Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.

Received 0... Displays the type and number of errors or other specific packets received. This information is displayed over three lines.

Output 0... Displays the type and number of packets sent out the interface. This information is displayed over three lines.

Rate information... Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.

Time since... Displays the time since the last change in the configuration of this interface.

Example

Dell# show interfaces port-channel 20
Port-channel 20 is up, line protocol is up (Failover-group 1 is down)
Hardware address is 00:01:e8:01:46:fa
Port-channel is part of failover-group 1
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel: Gi 2/5 Gi 2/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 00:00:00
Queueing strategy: fifo
44507301 packets input, 3563070343 bytes
Input 44506754 IP Packets, 0 Vlans 0 MPLS
41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-byte pkts
407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over 1023-byte pkts
Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
1218120 packets output, 100745130 bytes, 0 underruns
Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
1216142 IP Packets, 0 Vlans, 0 MPLS
0 throttles, 0 discarded
Rate info (interval 299 sec):
Input 01.50Mbits/sec, 2433 packets/sec
Output 00.02Mbits/sec, 4 packets/sec
Time since last interface status change: 00:22:34
Dell#

User Information

The following describes the show interfaces port-channel brief command shown in the following example.

Field Description
LAG Lists the port channel number.
Mode Lists the mode:
  • L3 — for Layer 3
  • L2 — for Layer 2
Status Displays the status of the port channel.
  • down — if the port channel is disabled (shutdown)
  • up — if the port channel is enabled (no shutdown)
Uptime Displays the age of the port channel in hours:minutes:seconds.
Ports Lists the interfaces assigned to this port channel.
(untitled) Displays the status of the physical interfaces (up or down).
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• In Layer 3 port channels, the primary port is not indicated.</td>
</tr>
</tbody>
</table>

**Example**

Dell# show interfaces port-channel 1 brief

<table>
<thead>
<tr>
<th>LAG Mode</th>
<th>Status</th>
<th>Uptime</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>up</td>
<td>00:00:08</td>
<td>Gi 3/1  (Up) *</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gi 3/2  (Down)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gi 3/3  (Up)</td>
</tr>
</tbody>
</table>

Dell#

**Related Commands**

- `show lacp` — display the LACP matrix.

### show port-channel-flow

Display an egress port in a given port-channel flow.

**Syntax**

```
show port-channel-flow outgoing-port-channel number incoming-interface interface {source-ip address destination-ip address} | {source-port number destination-port number} | {source-mac address destination-mac address {vlan vlan-id | ether-type}}
```

**Parameters**

- **outgoing-port-channel number**
  - Enter the keywords `outgoing-port-channel` then the number of the port channel to display flow information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- **incoming-interface interface**
  - Enter the keywords `incoming-interface` then the interface type and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- **source-ip address**
  - Enter the keywords `source-ip` then the IP source address in IP address format.

- **destination-ip address**
  - Enter the keywords `destination-ip` then the IP destination address in IP address format.

- **source-port number**
  - Enter the keywords `source-port` then the source port number. The range is from 1 to 65536. The default is `None`.

- **destination-port number**
  - Enter the keywords `destination-port` then the destination port number. The range is from 1 to 65536. The default is `None`.

- **source-mac address**
  - Enter the keywords `source-mac` then the MAC source address in the `nn:nn:nn:nn:nn:nn` format.

- **destination-mac address**
  - Enter the keywords `destination-mac` then the MAC destination address in the `nn:nn:nn:nn:nn:nn` format.

- **vlan vlan-id**
  - Enter the keywords `vlan` then the VLAN-id. The range is from 0 to 4094.
ether-type

Enter the keywords ether-type in the XX:XX format.

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Usage Information**

Because this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, not for routed packets (use the show ip flow command to display routed packets).

The `show port-channel-flow` command returns the egress port identification in a given port-channel if a valid flow is entered. A mismatched flow error occurs if MAC-based hashing is configured for a Layer 2 interface and you are trying to display a Layer 3 flow.

The output displays three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, the egress port of the first fragment.
- In the event of fragmented packets, the egress port of the subsequent fragments.

**NOTE:** In the `show port-channel-flow` command output, the egress port for an unknown unicast, multicast, or broadcast traffic is not displayed.

The following example shows the `show port-channel-flow outgoing-port-channel number incoming-interface interface source-mac address destination-mac address`

- Load-balance is configured for MAC
- Load-balance is configured for IP 4-tuple/2-tuple
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address

**Example**

```
Dell# show port-channel-flow outgoing-port-channel 1 incoming-interface gi 3/3 source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

Egress Port for port-channel 1, for the given flow, is Gi 13/2
```
Time Domain Reflectometer (TDR) Commands

TDR is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000 Base-T modules.

Important Points to Remember

- The interface and port must be enabled (configured—refer to the interface command) before running TDR. An error message is generated if you have not enabled the interface.
- The interface on the far-end device must be shut down before running TDR.
- Because TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

tdr-cable-test

Test the condition of copper cables on 100/1000 Base-T modules.

Syntax

```
tdr-cable-test interface
```

Parameters

- **interface**: Enter the keyword GigabitEthernet then the slot/port information for the 100/1000 Ethernet interface.

Defaults

None

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7.0.0</td>
<td>Introduced on the S5000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The interface must be enabled to run the test or an error message is generated:

```
Dell# tdr-cable-test gigabitethernet 5/2
%Error: Interface is disabled GI 5/2
```
Syslog messages are generated when the link flaps during TDR tests.

Related Commands

- `show tdr` — display the results of the TDR test.

### show tdr

Display the TDR test results.

**Syntax**

```
show tdr
```

**Parameters**

- `interface` Enter the keyword `GigabitEthernet` then the slot/port information for the 100/1000 Ethernet interface.

**Defaults**

None

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7.0.0</td>
<td>Introduced on the S5000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OK Status:</strong></td>
<td>TDR test is complete, no fault is detected on the cable, and the test is terminated.</td>
</tr>
<tr>
<td><strong>Terminated</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Length:</strong></td>
<td>92 (+/- 1) meters, Status: Shorted</td>
</tr>
<tr>
<td><strong>Open</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Status:</strong></td>
<td>Open</td>
</tr>
</tbody>
</table>


### Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Impedance Mismatch</td>
<td>There is an impedance mismatch in the cables.</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show tdr gigabitethernet 10/47
Time since last test: 00:00:02
Pair A, Length: OK Status: Terminated
Pair B, Length: 92 (+/- 1) meters, Status: Short
Pair C, Length: 93 (+/- 1) meters, Status: Open
Pair D, Length: 0 (+/- 1) meters, Status: Impedance Mismatch
```

### Related Commands

- `tdr-cable-test` — run the TDR test.

### UDP Broadcast Commands

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

- This feature is available only on the S4810, S4820T, S3048–ON, S4048–ON, Z9000 platforms.
- 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

**Command History**


**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
**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.

**Syntax**

```
ip udp-helper udp-port [udp-port-list]
```

To disable the UDP broadcast on a port, use the `no ip udp-helper udp-port [udp-port-list]` command.

**Parameters**

- **udp-port-list**
  
  (OPTIONAL) Enter up to 16 comma-separated UDP port numbers.

  **NOTE:** If you do not use this option, all UDP ports are considered by default.

**Defaults**

None

**Command Modes**

INTERFACE (conf-if)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>Pre-version 8.3.7.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you configure the `ip helper-address` command and `ip udp-helper udp-port` command, the behavior is that the UDP broadcast traffic with port numbers 67/68 is unicast relayed to the DHCP server per the `ip helper-address` configuration. This occurs regardless if the `ip udp-helper udp-port` command contains port numbers 67/68 or not.

If you only configure the `ip udp-helper udp-port` command, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the `udp-port-list`.

**Related Commands**

- `ip helper-address` — configure the destination broadcast or host address for the DHCP server.
show ip udp-helper

Display the configured UDP helpers on all interfaces.

Syntax  
show ip udp-helper

Defaults  
None

Command Modes  
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  
9.8(0.0P5)  
9.8(0.0P2)  
9.2(1.0)  
8.3.19.0  
8.3.11.1  
8.3.7.0  
Pre-version 8.3.7.0

Description
Introduced on the S4048-ON.
Introduced on the S3048-ON.
Introduced on the Z9500.
Introduced on the S4820T.
Introduced on the Z9000.
Introduced on the S4810.
Introduced on the E-Series.

Example
Dell# show ip udp-helper
---
Port     UDP  port  list
-----------------------------
Gi 10/2  656, 658
Gi 10/3  All

Related Commands
- debug ip udp-helper — enable debug and displays the debug information on a console.
- 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.
Internet Protocol Security (IPSec)

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — Connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — Confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — Algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes: Transport and Tunnel.

- **Transport** is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- **Tunnel mode** is used to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating virtual private networks (VPNs).

Transport mode provides IP packet payload protection using ESP. You can use ESP alone or in combination with AH to provide additional authentication. AH protects data from modification but does not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. The SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.

**NOTE:**
Due to performance limitations on the control processor, you cannot enable IPSec on all packets in a communication session.

Topics:

- crypto ipsec transform-set
- crypto ipsec policy
- management crypto-policy
- match
- session-key
- show crypto ipsec transform-set
- show crypto ipsec policy
- transform-set

**crypto ipsec transform-set**

Create a transform set, or combination of security algorithms and protocols, of cryptos.

**Syntax**

```
crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}
```
To delete a transform set, use the no crypto ipsec transform-set name {ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}} command.

Parameters

- **name**: Enter the name for the transform set.
- **ah-authentication**: Enter the keywords ah-authentication then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.
  - md5 — Use Message Digest 5 (MD5) authentication.
  - sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication.
  - null — Causes an encryption policy configured for the area to not be inherited on the interface.
- **esp-authentication**: Enter the keywords esp-authentication then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.
  - md5 — Use Message Digest 5 (MD5) authentication.
  - sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication.
  - null — Causes an encryption policy configured for the area to not be inherited on the interface.
- **esp-encryption**: Enter the keywords esp-encryption then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.
  - 3des — Use 3DES encryption.
  - cbc — Use CDC encryption.
  - des — Use DES encryption.
  - null — Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

Usage Information

- Both sides of the link must specify the same transform set.
- You can create up to 64 transform sets.

Example

Dell(conf)# do show crypto ipsec transform-set

<table>
<thead>
<tr>
<th>Transform-Set Name</th>
<th>refCnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>tsl</td>
<td>0</td>
</tr>
</tbody>
</table>
crypto ipsec policy

Create a crypto policy used by ipsec.

**Syntax**
n 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Enter the name for the crypto policy set.</td>
</tr>
<tr>
<td>seq-num</td>
<td>Enter the sequence number assigned to the crypto policy entry.</td>
</tr>
</tbody>
</table>

**Defaults**
None

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

**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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

match

Apply an match filter to the crypto policy.

Syntax

match seq-num tcp [source ip address | ipv6 address {mask} {source-port number}] [destination ip address | ipv6 address {mask} {destination-port number}]

To remove the match filter for the crypto map, use the no match seq-num tcp [source ip address | ipv6 address {mask} {source-port number}] [destination ip address | ipv6 address {mask} {destination-port number}] command.

Parameters

seq-num
Enter the match command sequence number.

source-ip-address | ipv6 address
Enter the keyword source then the IPv4 or IPv6 address for the source.

mask
Enter the mask prefix length in /nn format.

source-port number
Enter the source port number.

destination-port number
Enter the destination port number.

Defaults
None

Command Modes
CONFIG-CRYPTO-POLICY

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>
Version Description
9.2(1.0) Introduced on the Z9500.

Usage Information
- IPv4 addresses support only /32 mask types.
- IPv6 addresses support only /128 mask types.
- Configure match for bi-directional traffic for optimal routing.
- Only TCP is supported.

Example
match 0 tcp a::1 /128 0 a::2 /128 23
match 1 tcp a::1 /128 23 a::2 /128 0
match 2 tcp a::1 /128 0 a::2 /128 21
match 3 tcp a::1 /128 21 a::2 /128 0
match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32 23
match 5 tcp 1.1.1.1 /32 23 1.1.1.2 /32 0
match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32 21
match 7 tcp 1.1.1.1 /32 21 1.1.1.2 /32 0

session-key

Specify the session keys used in the crypto policy entry.

Syntax

```
session-key {inbound | outbound} {ah spi hex-key-string | esp spi encrypt hex-key-string auth hex-key-string}
```

To delete the session key information from the crypto policy, use the no session-key {inbound | outbound} {ah | esp} command.

Parameters

- **name**: Enter the name for the transform set.
- **inbound**: Specify the inbound session key for IPSec.
- **outbound**: Specify the outbound session key for IPSec.
- **ah**: Use the AH protocol when you select the AH transform set in the crypto policy.
- **esp**: Use the ESP protocol when you select the ESP transform set in the crypto policy.
- **spi**: Enter the security parameter index number.
- **hex-key-string**: Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.
- **encrypt**: Indicates the ESP encryption transform set key string.
- **auth**: Indicates the ESP authentication transform set key string.

Defaults

None

Command Modes

- CONF-CRYPTO-POLICY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(0.2) Introduced on the Z9000, S4810, and S4820T.
9.2(1.0) Introduced on the Z9500.

Example

Dell# show crypto ipsec transform-set

Transform-Set Name : dallas
Transform-Set refCnt : 0
AH Transform :
ESP Auth Transform :
ESP Encry Transform : 3des
Dell#
**show crypto ipsec policy**

Display the crypto policy configuration.

**Syntax**

`show crypto ipsec policy`

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf-crypto-policy)# do show crypto ipsec policy
Policy name : pol1
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.

**Syntax**

```
transform-set transform-set-name
```

To delete a transform set from the crypto policy, use the `no transform-set transform-set-name` command.

**Parameters**

- `transform-set-name` Enter the name for the crypto policy transform set.

**Defaults**

None

**Command Modes**

CONFIG-CRYPTO-POLICY

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
IPv4 Routing

The basic IPv4 commands are supported by Dell Networking OS on the platform.

Topics:
- arp
- arp backoff-time
- arp learn-enable
- arp max-entries
- 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
- 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 max-routes
- ip mtu
- ip name-server
- ip proxy-arp
- ip route
- ip source-route
- ip unreachable
- load-balance
- load-balance hg
- management route
- show arp
- show arp retries
To associate an IP address with a MAC address in the switch, use address resolution protocol (ARP).

**Syntax**
```
arp [vrf vrf-name] ip-address mac-address interface
```
To remove an ARP address, use the `no arp ip-address` command.

**Parameters**
- **vrf vrf-name**
  - Enter a VRF name to configure an ARP entry for that VRF. Use the VRF option after the keyword `arp` to configure a static arp on that particular VRF.
- **ip-address**
  - Enter an IP address in dotted decimal format.
- **mac-address**
  - Enter a MAC address in nnnn.nnnn.nnnn format.
- **interface**
  - (OPTIONAL) Enter any of the following keywords and slot/port or number information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
    - For a port channel interface, enter the keywords `port-channel` then a number.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
Version Description
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.4(0.0) Added support for VRF.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.2.1.0 Introduced on the E-Series.

Usage Information
You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.
You can use the vrf attribute of this command to create a static ARP entry on either a default or a non-default VRF. You cannot use this parameter to create any static ARPs corresponding to management VRFs. When a VRF is deleted using the no ip vrf command, all the static ARP configurations that belong to that VRF are removed automatically.

Related Commands
• clear arp-cache — clear dynamic ARP entries from the ARP table.
• show arp — display the ARP table.

arp backoff-time
Set the exponential timer for resending unresolved ARPs.

Syntax
arp backoff-time seconds

Parameters
seconds Enter the number of seconds an ARP entry is black-holed. The range is from 1 to 3600. The default is 30.

Defaults
30

Command Mode
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
This timer is an exponential backoff timer. Over the specified period, the time between ARP requests increases. This behavior reduces the potential for the system to slow down while waiting for a multitude of ARP responses.

**Related Commands**

- `show arp retries` — display the configured number of ARP retries.

**arp learn-enable**

Enable ARP learning using gratuitous ARP.

**Syntax**

```
arp learn-enable
```

**Defaults**

Disabled

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 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.
- 8.3.8.0  Introduced on the S4810.
Usage Information

In Dell Networking OS versions prior to 8.3.1.0, if a gratuitous ARP is received some time after an ARP request is sent, only RP2 installs the ARP information. For example:

1. At time t=0, Dell Networking OS sends an ARP request for IP A.B.C.D.
2. At time t=1, Dell Networking OS receives an ARP request for IP A.B.C.D.
3. At time t=2, Dell Networking OS installs an ARP entry for A.B.C.D only on RP2.

Beginning with Dell Networking OS version 8.3.1.0, when a gratuitous ARP is received, Dell Networking OS installs an ARP entry on all three CPUs.

arp max-entries

Enables you to configure the maximum number of ARP entries per VRF that are allowed for IPv4.

Syntax

arp max-entries [vrf vrf-name] max-number

Parameters

vrf vrf-name

Enter the name of a specific VRF for which you want to configure maximum number of ARP entries that IPv4 allows.

max-number

Enter the maximum number of ARP entries that a VRF RTM can hold. The range is from 0 to 65535.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.4.(0.0) Introduced on the S4810 and S4820T.

Usage Information

Use this command to specify the maximum number of ARP entries that the Route Table Manager can hold for a specific VRF. This command does not apply to the management VRFs.
arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Syntax  
arp retries number

Parameters  
number  Enter the number of retries. The range is from 1 to 20. The default is 5.

Defaults  
5

Command Modes  
CONFIGURATION

Command History  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information  
Retries are 20 seconds apart.

Related Commands  
- show arp retries — display 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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands
- show interfaces — display the ARP timeout value for all available interfaces.

**clear arp-cache**

Clear the dynamic ARP entries from a specific interface or optionally delete (no-refresh) ARP entries from the content addressable memory (CAM).

Syntax
```
clear arp-cache [vrf vrf-name | interface | ip ip-address] [no-refresh]
```

Parameters
- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf and then the name of the VRF to clear the ARP cache corresponding to that VRF.
- **interface** (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For the Management interface on the stack-unit, enter the keyword ManagementEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For an VLAN interface, enter the keyword vlan then a number.
For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

```
ip ip-address
```

(Optional) Enter the keyword `ip` then the IP address of the ARP entry you wish to clear.

```
no-refresh
```

(Optional) Enter the keywords `no-refresh` to delete the ARP entry from CAM. Or use this option with `interface` or `ip ip-address` to specify which dynamic ARP entries you want to delete.

**NOTE:** Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4094 VLANs on the E-Series (the prior limit was 2094).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### clear host

Remove one or all dynamically learned host table entries.

**Syntax**

```
clear host name
```
Parameters
- **name**: Enter the name of the host to delete. Enter * to delete all host table entries.

Command Modes
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### clear ip fib stack-unit

Clear all FIB entries in the specified stack unit (use this command with caution, refer to **Usage Information**.)

**Syntax**
```
clear ip fib stack-unit unit-number vrf vrf-name
```

**Parameters**
- **unit-number**: Enter the number of the stack unit.
- **vrf vrf-name**: Enter the keyword vrf followed by the name of the VRF to clear all FIB entries corresponding to that VRF.

Command Modes
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
clear ip route

Clear one or all routes in the routing table.

Syntax

```
clear ip route [vrf vrf-name] {* | ip-address mask}
```

Parameters

- `vrf vrf-name` (Optional) Enter the keyword `vrf` and then the name of the VRF to clear the routes corresponding to that VRF.
- `*` Enter an asterisk (*) to clear all learned IP routes.
- `ip-address mask` Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.4.(0.0) | Added support for VRF.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.9.1.0 | Introduced VRF on the E-Series.

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` — show FIB entries on a specified stack-unit.
Version | Description
--- | ---
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.2.1.1 | Introduced on the E-Series.

Usage Information

Use the \texttt{vrf vrf-name} attribute of this command to clear routes corresponding to either a specific VRF or the default VRF.

You cannot use this attribute to clear routes corresponding to a management VRF.

Related Commands

- \texttt{ip route} — assign an IP route to the switch.
- \texttt{show ip route} — view the routing table.
- \texttt{show ip route summary} — view a summary of the routing table.

\section*{clear tcp statistics}

Clear TCP counters.

Syntax

\texttt{clear tcp statistics [all | cp]}

Parameters

- all: Enter the keyword all to clear all TCP statistics maintained on all switch processors.
- cp: (OPTIONAL) Enter the cp to clear only statistics from the Control Processor.
- rp: (OPTIONAL) Enter the keyword rp to clear only the statistics from Route Processor.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
debug arp

View information on ARP transactions.

Syntax

`debug arp [interface] [count value]`

To stop debugging ARP transactions, use the `no debug arp` command.

Parameters

- **interface**: (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

- **count value**: (OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534.

Defaults

None

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

- 9.8(1.0) Introduced on the Z9100-ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Introduced on the S6000-ON.
- 9.2(1.0) Introduced on the Z9500.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.11.1 Introduced on the Z9000.
- 8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
- 8.3.7.0 Introduced on the S4810.
debug ip dhcp

Enable debug information for dynamic host configuration protocol (DHCP) relay transactions and display the information on the console.

Syntax
debug ip dhcp

To disable debug, use the no debug ip dhcp command.

Defaults
Debug disabled

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.4.1.0 Introduced on the E-Series.

Example
Dell# debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface
14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface
14.4.4.1 BOOTP Reply, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
Dell#

Related Commands
• ip helper-address – specify the destination broadcast or host address for the DHCP server request.
• ip helper-address hop-count disable – disable the hop-count increment for the DHCP relay agent.

debug ip icmp

View information on the internal control message protocol (ICMP).

Syntax
debug ip icmp [interface] [count value]
To disable debugging, use the no debug ip icmp command.

Parameters

interface (OPTIONAL) Enter the following keywords and the interface information:
• For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
• For the Management interface on the stack-unit, enter the keyword ManagementEthernet then the slot/port information.
• For a port channel interface, enter the keywords port-channel then a number.
For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

For a VLAN interface, enter the keyword `count` then a number from 1 to 65534. The default is `Infinity`.

**Command Modes**

* EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4094 VLANs on the E-Series (the prior limit was 2094).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the <code>count</code> option.</td>
</tr>
</tbody>
</table>

**Usage Information**

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

**debug ip packet**

View a log of IP packets sent and received.

**Syntax**

debug ip packet [access-group name] [count value] [interface]
To disable debugging, use the `no debug ip packet [access-group name] [count value] [interface]` command.

**Parameters**

- **access-group name** Enter the keyword `access-group` then the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.
- **count value** (OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is `Infinity`.
- **interface** (OPTIONAL) Enter the following keywords and the interface information:
  - For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4094 VLANs on the E-Series (the prior limit was 2094).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added the <code>access-group</code> option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Added the <code>count</code> option.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `debug ip packet` command in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>s=</td>
<td>Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>d=</td>
<td>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.</td>
</tr>
<tr>
<td>len</td>
<td>Displays the packet’s length.</td>
</tr>
<tr>
<td>sending, rcvd, fragment, sending broad/multicast proto, unroutable</td>
<td>The last part of each line lists the status of the packet.</td>
</tr>
<tr>
<td>TCP src=</td>
<td>Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.</td>
</tr>
<tr>
<td>UDP src=</td>
<td>Displays the source and destination ports for the UDP packets.</td>
</tr>
<tr>
<td>ICMP type=</td>
<td>Displays the ICMP type and code.</td>
</tr>
<tr>
<td>IP Fragment</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Example**

IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 1/1), len 54, sending
TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 1/1), d=10.1.2.62, len 40, rcvd
TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 1/1), len 226, sending
TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 1/1), d=10.1.2.255, len 78, rcvd
UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 1/1), len 1500, sending fragment
IP Fragment, Ident = 4741, fragment offset = 0
ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 1/1), len 1500, sending fragment
IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Gi 4/11), len 64, sending broad/multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Gi 4/11), len 28, sending broad/multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
ICMP type=8, code=0

**Usage Information**

To stop packets from flooding the user terminal when debugging is turned on, use the count option.

The access-group option supports only the equal to (eq) operator in TCP ACL rules. Port operators not equal to (neq), greater than (gt), less than (lt), or range are not supported in access-group option (refer to the following example). ARP packets (arp) and Ether-type (ether-type) are also not supported in the access-group option. The entire rule is skipped to compose the filter.

The access-group option pertains to:

- IP protocol number: from 0 to 255
- Internet control message protocol (icmp) but not the ICMP message type (from 0 to 255)
- Any internet protocol (ip)
- Transmission Control Protocol (tcp) but not on the rst, syn, or urg bits
- User Datagram Protocol (udp)
In the case of ambiguous access control list rules, the debug ip packet access-control command is disabled. A message appears identifying the error (refer to the Example below).

Example (Error Messages)

Dell# debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

Dell#00:10:45: %RPM0-P:CP
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not supported in access-list debug, access-list debugging is turned off
Dell#

**ip address**

Assign a primary and secondary IP address to the interface.

**Syntax**

```
ip address ip-address mask [secondary]
```

To delete an IP address from an interface, use the no ip address [ip-address] command.

**Parameters**

- **ip-address**
  - Enter an IP address in dotted decimal format.

- **mask**
  - Enter the mask of the IP address in slash prefix format (for example, /24).

- **secondary**
  - (OPTIONAL) Enter the keyword secondary to designate the IP address as the secondary address.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
ip directed-broadcast

Enables the interface to receive directed broadcast packets.

Syntax
ip directed-broadcast

To disable the interface from receiving directed broadcast packets, use the no ip directed-broadcast command.

Defaults
Disabled (that is, the interface does not receive directed broadcast packets)

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
**ip domain-list**

Configure names to complete unqualified host names.

**Syntax**

```
ip domain-list name
```

To remove the name, use the no ip domain-list name command.

**Parameters**

- `name` Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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` — specify a DNS server.

**ip domain-lookup**

To address resolution (that is, DNS), enable dynamic host-name.

**Syntax**
```
ip domain-lookup
```

To disable DNS lookup, use the `no ip domain-lookup` command.

**Defaults**
Disabled.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
To fully enable DNS, also specify one or more domain name servers with the `ip name-server` command.

Dell Networking OS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

To view current bindings, use the `show hosts` command.

**Related Commands**
- `ip name-server` — specify a DNS server.
show hosts — view the current bindings.

ip domain-name

Configure one domain name for the switch.

Syntax

```
ip domain-name name
```  

To remove the domain name, use the `no ip domain-name` command.

Parameters

- `name`  
  Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults

Not configured.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.

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` — configure additional names.

**ip helper-address**

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

**Syntax**

```
ip helper-address ip-address
```

To remove a DHCP server address, use the **no ip helper-address** command.

**Parameters**

- `ip-address` Enter an IP address in dotted decimal format (A.B.C.D).

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can add multiple DHCP servers by entering the **ip helper-address** command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.
Dell Networking OS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and Dell Networking OS forwards to the client with source port=67, destination port=68.

**ip helper-address hop-count disable**

Disable the hop-count increment for the DHCP relay agent.

### Syntax

```
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

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced for the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through Dell Networking OS. If the incoming boot request already has a non-zero hops field, the message is relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

### Related Commands

- `ip helper-address` — specify the destination broadcast or host address for DHCP server requests.
- `show running-config` — display the current configuration and changes from the default values.
ip host

Assign a name and an IP address to the host-to-IP address mapping table.

Syntax

```
ip host name ip-address
```

To remove an IP host, use the `no ip host name [ip-address]` command.

Parameters

- **name**: Enter a text string to associate with one IP address.
- **ip address**: Enter an IP address, in dotted decimal format, to be mapped to the name.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for the E-Series.</td>
</tr>
</tbody>
</table>

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`.

**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 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.

For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.

For a port channel interface, enter the keywords `port-channel` then a number.

For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
</tbody>
</table>

**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 gigabitethernet 1/1
Dell(conf)#
```
ipv6 icmp source-interface

Enable the ICMP error and unreachable messages to be sent with the source interface IP address, such as the loopback address, instead of the hops of the preceding devices along the network path to be used for easy debugging and diagnosis of network disconnections and reachability problems with IPv6 packets.

Syntax
ipv6 icmp source-interface interface

Parameters

interface
Enter one of the following keywords and slot/port or number information:

- For a Management Ethernet interface, enter the keyword managementethernet.
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.3(0.0) Introduced on the S4810, S4820T, S6000, and Z9000 platforms.

Usage Information
You can enable the mechanism to configure the source or the originating interface from which the packet (the device that generates the ICMP error messages) is received by the switch to send the loopback address instead of its source IP address to be used in the ICMP unreachable messages and in the traceroute command output. The loopback address must be unique in a particular domain.

In network environments that contain a large number of devices, ranging up to thousands of systems, and with each device configured for equal-cost multipath (ECMP) links, you cannot effectively and optimally use the traceroute and ping applications to examine the network reachability and identify any broken links for diagnostic purposes. In such cases, if the reply that is obtained from each hop on the network path contains the IP address of
the adjacent, neighboring interface from which the packet is received, it is difficult
to employ the ping and traceroute utilities. You can enable the ICMP unreachable messages to contain the loopback address of the source
device instead of the previous hop's IP address to be able to easily and quickly identify the device and devices
along the path because the DNS server maps the loopback IP address to the hostname and does not translate the
IP address of every interface of the switch to the hostname

Example

Dell(conf)# ipv6 icmp source-interface gigabitethernet 1/1
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced for the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.
ip max-routes

Enables you to configure the maximum number of protocol routes per VRF that are allowed for IPv4.

Syntax

ip max-routes [vrf vrf-name] max-number

Parameters

vrf vrf-name Enter the keyword vrf and then the name of the VRF for which you want to configure maximum number of protocol routes that IPv4 allows.

max-number Enter the maximum number of protocol routes that a VRF RTM can hold. The range is from 0 to 7500.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version 9.4.(0.0) Introduced on the S4810 and S4820T.

Usage Information

Use this command to specify the maximum number of protocol routes that the Route Table Manager can hold for a specific VRF. This command does not apply to the management VRFs.

Related Commands

- show ip route — view the switch routing table.
- show ipv6 route — display the IPv6 routes.

ip mtu

Set the IP MTU (frame size) of the packet the RPM transmits for the line card interface. If the packet must be fragmented, Dell Networking OS sets the size of the fragmented packets to the size specified in this command.

Syntax

ip mtu value

To return to the default IP MTU value, use the no ip mtu command.

Parameters

value Enter the maximum MTU size if the IP packet is fragmented. The range is from 576 to 9234. The default is 1500 bytes.

Defaults

1500 bytes

Command Modes

INTERFACE (Gigabit Ethernet and 10-Gigabit Ethernet interfaces)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Verison | Description
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
6.1.1.0 | Introduced on the E-Series.

**Usage Information**

When you enter the `no mtu` command, Dell Networking OS reduces the ip mtu value to 1536 bytes. To return the IP MTU value to the default, use the `no ip mtu` command.

Starting with Dell Networking OS Release 9.2(0.2), the `ip mtu` command is not supported to configure the IP MTU value that is used when the IP packet is fragmented. Instead of having to configure the IP MTU value, this value is automatically computed by the software when you configure an interface. As a result, the ip mtu command is not available for configuration. However, you can continue to specify the link MTU value by using the mtu command.

Compensate for Layer 2 header when configuring link MTU on an Ethernet interface or Dell Networking OS may not fragment packets. If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (the `ip mtu` command) must be enough bytes to include for the Layer 2 header.

**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 of 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 describes the difference between Link MTU and IP MTU.

<table>
<thead>
<tr>
<th>Layer 2 Overhead</th>
<th>Difference between Link MTU and IP MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet (untagged)</td>
<td>18 bytes</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Tag 22 bytes</td>
</tr>
<tr>
<td>Untagged Packet with VLAN-Stack Header</td>
<td>22 bytes</td>
</tr>
</tbody>
</table>
Layer 2 Overhead
Tagged Packet with VLAN-Stack Header

Difference between Link MTU and IP MTU

Tagged Packet with VLAN-Stack Header

26 bytes

Related Commands

- mtu — set the link MTU for an Ethernet interface.

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 to 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100–ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

8.1.1.0 Introduced on the E-Series.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

pre-6.1.1.0 Introduced on the E-Series.
Usage Information

Dell Networking OS does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

You can separately configure both IPv4 and IPv6 domain name servers.

In a dual stack setup, the system sends both A (request for IPv4 — RFC 1035) and AAAA (request for IPv6 — RFC 3596) record requests to a DNS server even if only the ip name-server command is configured.

ip proxy-arp

Enable proxy ARP on an interface.

Syntax

ip proxy-arp

To disable proxy ARP, use the no ip proxy-arp command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- show ip interface — display the interface routing status and configuration.
**ip route**

Assign a static route to the switch.

**Syntax**

```
ip route [vrf vrf-name] ip-address mask {ip-address | interface [ip-address]} [distance] [permanent] [tag tag-value] [vrf vrf-name] [weight weight-value]
```

To delete a specific static route, use the `no ip route destination mask` command.

To delete all routes matching a certain route, use the `no ip route destination mask` command.

**Parameters**

- **vrf vrf-name**  
  (Optional) Enter the keyword `vrf` and then the name of the VRF to configure a static route corresponding to that VRF. Use this VRF option after the `ip route` keyword to configure a static route on that particular VRF.

- **destination**  
  Enter the IP address in dotted decimal format of the destination device.

- **mask**  
  Enter the mask in the slash prefix format (/x) of the destination IP address.

- **ip-address**  
  Enter the IP address of the forwarding router in dotted decimal format.

- **interface**  
  Enter one of the following keyword followed by the interface information:

  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a Null interface, enter the keyword null then the Null interface number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
  - For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.

If you configure a static IPv6 route using an egress interface and enter the ping command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the ping command to detect the destination address.

- **interface ip-address**  
  Enter the keyword `interface` then the IP address.

- **distance**  
  (Optional) Enter the value of the distance metric assigned to the route. The range is from 1 to 255.

- **permanent**  
  (Optional) Enter the keyword `permanent` to specify that the route must not be removed even if the interface assigned to that route goes down. The route must be currently active to be installed in the routing table. If you disable the interface, the route is removed from the routing table.
tag tag-value  (OPTIONAL) Enter the keyword tag then a number to assign to the route. The range is from 1 to 4294967295.

vrf vrf-name  Enter the keyword vrf followed by the name of the VRF. Use this VRF option after the next hop to specify which VRF the next hop belongs to. This setting is used in route leaking cases. See “R”oute Leaking VRFs” in the Virtual Routing and Forwarding (VRF) section of the Configuration guide.

weight weight-value  Enter the keyword weight followed by a weight value. The range is from 0 to 255.

NOTE: Weight for a static route can be added only for the destination address and not for the route pointing to destination a interface.

Defaults  Not configured.

Command Modes CONFIGURATION

Command History  This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  Description
9.8(1.0)  Introduced on the Z9100–ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)  Introduced on the S6000-ON.
9.4.(0.0)  Added support for VRF.
9.2(1.0)  Introduced on the Z9500.
9.0.2.0  Introduced on the S6000.
9.2.(0.0)  Added support for tunnel interface type.
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.5.1.0  Added support for 4-port 40G line cards on the E-Series.
8.3.7.0  Introduced on the S4810.
8.2.1.0  Added support for 4094 VLANs on the E-Series (the prior limit was 2094).
8.1.1.0  Introduced on the E-Series.
7.9.1.0  Introduced VRF on the E-Series.
7.6.1.0  Introduced on the S-Series.
7.5.1.0  Introduced on the C-Series.
pre-6.1.1.0  Introduced on the E-Series.

Usage Information  Using the following example of a static route: ip route 33.33.33.0 /24 tengigabitethernet 1/1 172.31.5.43

• The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if tengig 1/1 has an ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, Dell Networking OS installs the static route.
• When the interface goes down, Dell Networking OS withdraws the route.
• When the interface comes up, Dell Networking OS re-installs the route.
• When recursive resolution is “broken,” Dell Networking OS withdraws the route.
When recursive resolution is satisfied, Dell Networking OS re-installs the route.

You can specify a weight for an IPv4 or IPv6 static route. If the weight value of a path is 0, then that path is not used for forwarding when weighted ECMP is in effect. Also, if a path corresponding to a static route (destination) has a non-zero weight assigned to it and other paths do not have any weight configured, then regular ECMP is used for forwarding.

You can specify the weight value only to destination address and not on the egress port.

A route is considered for weighted ECMP calculations only if each paths corresponding to that route is configured with a weight.

You cannot use the VRF attribute of this command to configure routes in a management VRF. When a specific VRF is deleted, all the configured static routes corresponding to that VRF are automatically removed.

Example

Dell(conf)# ip route 1.1.1.0/24 4.4.4.2 weight 100
Dell(conf)# ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)# do show running-config | grep route
ip route 1.1.1.0/24 4.4.4.2 weight 100
ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)# ip route vrf test 1.1.1.0/24 4.4.4.2 weight 100
Dell(conf)# ip route vrf test 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#
Dell(conf)# do show running-config | grep route
ip route vrf test 1.1.1.0/24 4.4.4.2 weight 100
ip route vrf test 1.1.1.0/24 6.6.6.2 weight 200

Related Commands

- show ip route — view the switch routing table.

**ip source-route**

Enable Dell Networking OS to forward IP packets with source route information in the header.

**Syntax**

```
ip source-route
```

To drop packets with source route information, use the `no ip route-source` command.

**Defaults**

Enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(10)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
ip unreachables

Enable the generation of internet control message protocol (ICMP) unreachable messages.

Syntax
ip unreachables
To disable the generation of ICMP messages, use the no ip unreachables command.

Defaults
Disabled.

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.
load-balance

By default, for C-Series and S-Series, Dell Networking OS uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the load-balance command.

Syntax

load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port [enable]}
To return to the default setting (IP 4-tuple), use the no load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port [enable]} command.

Parameters

ip-selection (dest-ip | source-ip)
- dest-ip — Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- source-ip — Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

mac (dest-mac | source-dest-mac | source-mac)
- dest-mac — Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- source-dest-mac — Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- source-mac — Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

tcp-udp enable
- enable — Takes the TCP/UDP source and destination ports into consideration when doing hash computations. This option is enabled by default.

Ingress-port enable
- enable — Takes the source port into consideration when doing hash computations. This option is disabled by default.

Defaults
IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.10.0 | Added the `ingress-port` parameter for the S4810.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.

Usage Information
By default, 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**
```
```

**Parameters**
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.
IPv4 Routing

MAC [source-mac | source-port-id | source-module-id | dest-mac | dest-port-id | dest-module-id | vlan | ethertype | source-dest-mac]

To use MAC key fields in hash computation, enter the keyword mac then one of the parameters:

- source-mac — Use source-mac field in hash calculation.
- source-port-id — Use src-port-id field in hash calculation.
- source-module-id — Use src-module-id field in hash calculation.
- dest-mac — Use dest-mac field in hash calculation.
- dest-port-id — Use dest-port-id field in hash calculation.
- dest-module-id — Use dest-module-id field in hash calculation.
- vlan — Use vlan field in hash calculation.
- ethertype — Use Ethertype field in hash calculation.
- source-dest-mac — Use SMAC and DMAC fields in hash calculation.

Tunnel [ipv4-over-ipv4 | ipv4-over-gre-ipv4 | mac-in-mac]

To use tunnel key fields in hash computation, enter the keyword tunnel then one of the parameters:

- ipv4-over-ipv4 — Use ipv4-over-ipv4 field in hash calculation.
- ipv4-over-gre-ipv4 — Use ipv4-over-gre-ipv4 field in hash calculation.
- mac-in-mac — Use mac-in-mac field in hash calculation.

Defaults
IP selection 5-tuples (source-ip dest-ip vlan protocol L4-source-port L4-dest-port).

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
management route

Configure a static route that points to the Management interface or a forwarding router.

Syntax

```
management route {ip-address mask | ipv6-address 1.1.1.1prefix-length}
(forwarding-router-address | managementethernet| vlan | gigabitethernet | tengigabitethernet)
```

To remove a static route, use the `no management route` command.

Parameters

- **ip-address mask**: Enter an IP address (dotted decimal format) and mask (/prefix format) of the destination subnet.
- **ipv6-address prefix-length**: Enter an IPv6 address (x:x:x:x::x format) and mask (/prefix format) of the destination subnet. Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format.
  
  The range is from /0 to /128.

  **NOTE**: The :: notation specifies successive hexadecimal fields of zeros.

- **forwarding-router-address**: Enter an IP address (dotted decimal format) or an IPv6 address (x:x:x:x::x format) of a forwarding router.
- **managementethernet**: Enter the keyword managementethernet for the Management interface on the Primary RPM.
- **vlan**: Enter the keyword vlan to specify a vlan interface.
- **gigabitethernet**: Enter the keyword gigabitethernet to specify a one Gigabit Ethernet interface.
- **tengigabitethernet**: Enter the keyword tengigabitethernet to specify a ten Gigabit Ethernete interface.

Defaults

Not configured.

Command Modes

- CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for forty gigabit, vlan, and tengigabit ethernet interfaces. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000 and added support for IPv6.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

#### Usage Information

When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.

#### Related Commands

- `interface ManagementEthernet` — configure the Management port on the system (either the Primary or Standby RPM).
- `speed (Management interface)` — set the speed for the Management interface.

### show arp

Display the ARP table.

#### Syntax

```
show arp [vrf vrf-name] [interface interface | ip ip-address [mask] | macaddress mac-address [mac-address-mask]] [retries] [static | dynamic] [inspection {database | statistics}] [summary]
```

#### Parameters

- **vrf vrf-name** *(OPTIONAL)* Enter the keyword `vrf` and then the name of the VRF.

  **NOTE:** Use this attribute to start a BGP instance for either a specific address family corresponding to the default VRF or an IPv4 address family corresponding to a non-default VRF.

- **interface interface** *(OPTIONAL)* Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

- **ip ip-address mask** *(OPTIONAL)* Enter the keyword `ip` then an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (/x).

- **inspection** *(OPTIONAL)* Enter the keyword `inspection` with one of the following keywords to view ARP entries:
  - `database` — view a list of ARP entries learned using DAI
  - `statistics` — view DAI statistics

---

**IPv4 Routing**  |  729
**macaddress mac-address mask**


**static**

(Optional) Enter the keyword `static` to view entries entered manually.

**retries**

(Optional) Enter the keyword `retries` to show the number of ARP retries before a 20-second back off.

**dynamic**

(Optional) Enter the keyword `dynamic` to view dynamic entries.

**summary**

(Optional) Enter the keyword `summary` to view a summary of ARP entries.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF and added usage information for the <code>clear arp-cache</code> command.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added support for 4094 VLANs on the E-Series (the prior limit was 2094).</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Augmented to display local ARP entries learned from private VLANs (PVLANs).</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Private VLAN (PVLAN)).

If you have entered the `clear arp-cache` command to remove a large number of ARP entries and the command is still being processed in the background, an error message display if you attempt to enter the `show arp` command:

```
Clear arp in-progress. Please try after sometime!
```

The following describes the `show arp` command shown in the following example.
### Description

**Protocol**
Displays the protocol type.

**Address**
Displays the IP address of the ARP entry.

**Age(min)**
Displays the age (in minutes) of the ARP entry.

**Hardware Address**
Displays the MAC address associated with the ARP entry.

**Interface**
Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.

**VLAN**
Displays the VLAN ID, if any, associated with the ARP entry.

**CPU**
Lists which CPU the entries are stored on.

### Example

```
Dell> show arp
Protocol  Address  Age(min)  Hardware Address  Interface  VLAN  CPU
-------------------------------------------------------------
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
Internet  192.2.1.254 1  00:00:c0:02:01:02  Gi 2/13 -  CP
```

### Example (Private VLAN)

> **NOTE:** In this example, Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN. Line 2 shows primary VLAN 10.

```
Dell# show arp
Protocol  Address  Age(min)  Hardware Address  Interface  VLAN  CPU
---------------------------------------------------------------
Internet 5.5.5.1       -  00:01:e8:43:96:5e  -      Vl 10 pv 200 CP
Internet 5.5.5.10      -  00:01:e8:44:99:55  -      Vl 10        CP
Internet 10.1.2.4      1  00:01:e8:d5:9e:e2  Ma 1/1 -            CP
Internet 10.10.10.4    1  00:01:e8:d5:9e:e2  Ma 1/1 -            CP
Internet 10.1.127.53   1  00:01:e8:d5:9e:e2  Ma 1/1 -            CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2  Ma 1/1 -            CP
Internet 133.33.33.4   1  00:01:e8:d5:9e:e2  Ma 1/1 -            CP
```

### Usage Information

The following describes the `show arp summary` command shown in the following example.

### Description

**Total Entries**
Lists the total number of ARP entries in the ARP table.

**Static Entries**
Lists the total number of configured or static ARP entries.

**Dynamic Entries**
Lists the total number of learned or dynamic ARP entries.

**CPU**
Lists which CPU the entries are stored on.

### Example (Summary)

```
Dell# show arp summary
TotalEntries Static Entries Dynamic Entries CPU
---------------------------------------------
83          0            83                CP
Dell#
```
show arp retries

Display the configured number of ARP retries.

Syntax

```
show arp retries
```

Command Modes

```
  • EXEC
  • EXEC Privilege
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.8(1.0)  Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)  Introduced on the S6000-ON.
9.2(1.0)  Introduced on the Z9500.
9.0.2.0  Introduced on the S6000.
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.3.1.0  Introduced.
```

Related Commands

```
  • arp retries — set 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
```

show arp retries

Display the configured number of ARP retries.

Syntax

```
show arp retries
```

Command Modes

```
  • EXEC
  • EXEC Privilege
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.8(1.0)  Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)  Introduced on the S6000-ON.
9.2(1.0)  Introduced on the Z9500.
9.0.2.0  Introduced on the S6000.
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.3.1.0  Introduced.
```

Related Commands

```
  • arp retries — set 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
```

show hosts

View the host table and DNS configuration.
EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Added support for IPv6 addresses.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show hosts command in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default domain...</td>
<td>Displays the domain name (if configured).</td>
</tr>
<tr>
<td>Name/address lookup...</td>
<td>States if DNS is enabled on the system.</td>
</tr>
<tr>
<td>Name servers are...</td>
<td>Lists the name servers, if configured.</td>
</tr>
<tr>
<td>Host</td>
<td>Displays the host name assigned to the IP address.</td>
</tr>
<tr>
<td>Flags</td>
<td>Classifies the entry as one of the following:</td>
</tr>
<tr>
<td></td>
<td>• perm — the entry was manually configured and will not time out</td>
</tr>
<tr>
<td></td>
<td>• temp — the entry was learned and will time out after 72 hours of inactivity.</td>
</tr>
<tr>
<td></td>
<td>Also included in the flag is an indication of the validity of the route:</td>
</tr>
<tr>
<td></td>
<td>• ok — the entry is valid.</td>
</tr>
<tr>
<td></td>
<td>• ex — the entry expired.</td>
</tr>
<tr>
<td></td>
<td>• ?? — the entry is suspect.</td>
</tr>
<tr>
<td>TTL</td>
<td>Displays the amount of time until the entry ages out of the cache. For dynamically learned entries only.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays IP as the type of entry.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the IP addresses assigned to the host.</td>
</tr>
</tbody>
</table>
Example

Dell# show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set

<table>
<thead>
<tr>
<th>Host</th>
<th>Flags</th>
<th>TTL</th>
<th>Type</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ks</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td>4200-1</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.68.69.2</td>
</tr>
<tr>
<td>1230-3</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.68.99.2</td>
</tr>
<tr>
<td>ZZr</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.71.18.2</td>
</tr>
<tr>
<td>210-3</td>
<td>(perm, OK)</td>
<td>-</td>
<td>IP</td>
<td>192.71.23.1</td>
</tr>
</tbody>
</table>

Dell#

Related Commands
- traceroute — view the DNS resolution.
- ip host — configure a host.

show ip cam stack-unit

Display CAM entries for a port-pipe of a stack-unit on a S-Series or Z-Series switch.

Syntax

show ip cam stack-unit {stack-unit-number} {port-set {pipe-number} | vrf vrf-name {ip-address mask [longer-prefixes [ecmp-group detail]]}| ecmp-group {detail | member-info [detail [group-index index-number]]]| summary}

Parameters

- **stack-unit-number**
  Enter the stack-unit ID. The unit ID range is from 1 to 6.

- **port-set pipe-number**
  Enter the keyword port-set then the number of the stack unit’s port-pipe. The unit ID range is from 0 to 0.

- **vrf vrf-name**
  Enter the keyword vrf followed by the name of the VRF to display CAM entries corresponding to that VRF.

- **network mask [longer-prefixes [ecmp-group detail]]**
  (OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. You can enter one of the following keywords to filter results.

  - Enter the keyword longer-prefixes to view routes with a common prefix.
  - Enter the keyword ecmp-group detail to view the ECMP group index.

- **ecmp-group (detail | member-info [detail [group-index index-number]]))**
  (OPTIONAL) Enter the keyword ecmp-group then one of the following keywords to filter results.

  - Enter the keyword detail to view the ECMP group index.
  - Enter the keyword member-info to view the member information for the ECMP group.
  - Enter the keyword member-info detail to view detailed ECMP membership and n-hop information.
  - Enter the keyword group-index then the index number to show ECMP membership per group. The range is from 0 to 1022.

- **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
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

## Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added support for up to seven stack members.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

## Usage Information

The following describes the **show ip cam** command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>Displays the destination route of the index.</td>
</tr>
<tr>
<td><strong>EC</strong></td>
<td>Displays 1 if the route is an ECMP route. Else, displays 0.</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>This is the CPU bit. If it displays 1, then it indicates that a packet hitting this entry will be forwarded to the CPU.</td>
</tr>
<tr>
<td><strong>V Id</strong></td>
<td>Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.</td>
</tr>
<tr>
<td><strong>Mac Addr</strong></td>
<td>Displays the next-hop router's MAC address.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Displays the egress interface.</td>
</tr>
<tr>
<td></td>
<td>• CP = control processor</td>
</tr>
<tr>
<td></td>
<td>• Gi = Gigabit Ethernet interface</td>
</tr>
<tr>
<td></td>
<td>• Te = 10-Gigabit Ethernet interface</td>
</tr>
</tbody>
</table>

### Example

```
Dell# show ip cam stack-unit 3 po 0 1.1.1.0/24 longer-prefixes

Destination           EC  C   VId  Mac-Addr             Port  
----------------------- ------ ---- ---- ------------------ ------ 
1.1.1.2/32             0  0    3000 00:05:00:00:00:02  Gi 3/44  
1.1.1.1/32             0  1    0    00:00:00:00:00:00  CP   
1.1.1.0/24             0  1    0    00:00:00:00:00:00  CP   
```

### Example (ECMP-Group)

```
Dell# show ip cam stack-unit 3 po 0 1.1.1.0/24 longer-prefixes

Destination       EC  C   VId   Mac-Addr             Port  
----------------- ------ ---- ---- ------------------ ------ 
1.1.1.2/32        0  0    1000 00:01:00:00:00:00:02  Gi 3/44  
2.1.1.2/32        0  0    20   00:03:00:00:00:00:00  Po 10   
2.1.1.1/32        0  1    0    00:00:00:00:00:00:00  CP   
1.1.1.1/32        0  1    0    00:00:00:00:00:00:00  CP   
2.1.1.0/24        0  1    0    00:00:00:00:00:00:00  CP   
1.1.1.0/24        0  1    0    00:00:00:00:00:00:00  CP   
100.1.1.0/24       1  0    20   00:03:00:00:00:00:02  Po 10   
```
Example (Member-Info)

```
Dell# show ip cam stack-unit 3 po 0 ecmp-group member-info detail

<table>
<thead>
<tr>
<th>Group Index</th>
<th>Member Count</th>
<th>Mac-Addr</th>
<th>Port</th>
<th>VLan ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2</td>
<td>00:03:00:00:00:02</td>
<td>Po 10</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>00:01:00:00:00:02</td>
<td>Gi 3/42</td>
<td>1000</td>
</tr>
</tbody>
</table>

Dell#
```
Version Description
8.3.7.0 Introduced on the S4810.
7.7.1.0 Added support for up to seven stack members.
7.6.1.0 Introduced on the S-Series.

Usage Information
The following describes the show ip fib stack-unit command shown in the following example.

Field Description
Destination Lists the destination IP address.
Gateway Displays either the word “direct” and an interface for a directly connected route or the remote IP address used to forward the traffic.
First-Hop Displays the first hop IP address.
Mac-Addr Displays the MAC address.
Port Displays the egress-port information.
VId Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
EC Displays the number of ECMP paths.

If weighted ECMP is enabled, then the show ip fib stack-unit command display a new column named W-EC (Weighted ECMP). This column displays either a value of 1 or 0 depending on whether or not a route is assigned with a weight.

Example
Dell# show ip fib stack-unit 1
Destination Gateway First-Hop Mac-Addr Port VId EC
-----------------------------------------------------------------------
1.1.1.2/32 via 1.1.1.2, Vl 1000 1.1.1.2 00:01:00:00:00:02 Gi 3/42 1000 0
2.1.1.2/32 via 2.1.1.2, Vl 20 2.1.1.2 00:03:00:00:00:02 Po 10 20 0
0.0.0.0/0 - - - - CP 0 0 - -
1.1.1.0/24 Direct, Vl 1000 0.0.0.0 00:00:00:00:00:00 CF 0 0
1.1.1.1/32 via 127.0.0.1 127.0.0.1 00:00:00:00:00:00 CF 0 0
2.1.1.0/24 Direct, Vl 20 0.0.0.0 00:00:00:00:00:00 CF 20 0
2.1.1.1/32 via 127.0.0.1 127.0.0.1 00:00:00:00:00:00 CF 0 0
100.1.1.0/24 via 1.1.1.2, Vl 1000 1.1.1.2 00:01:00:00:00:02 Gi 3/42 1000 1
100.1.1.0/24 via 2.1.1.2, Vl 20 2.1.1.2 00:03:00:00:00:02 Po 10 20 1
Dell# show ip route
S 10.1.1.0/24 via 1.1.1.2, Vl 10
via 2.1.1.2, Vl 20
S 20.1.1.0/24 via 3.1.1.2, Vl 30
S 100.1.1.0/24 via 10.1.1.0, weight 7
via 20.1.1.0, weight 1

Example (Show command output with Weighted ECMP Enabled)
Dell# show ip fib stack-unit 1
Destination Gateway First-Hop Mac-Addr Port VId EC RC W
-----------------------------------------------------------------------
0.0.0.0/0 - - - - CP 0 0 - -
1.1.1.0/24 Direct, Lo 0 0.0.0.0 00:00:00:00:00:00 CP 0 0 - -
1.1.1.1/32 via 127.0.0.1 127.0.0.1 00:00:00:00:00:00 CP 0 0 - -

Example
The RC and W columns in the show output appear only if the weighted ECMP is enabled using the ip ecmp weighted command.

Related Commands
- clear ip fib stack-unit — clear FIB entries on a specified stack-unit.
- ip ecmp weighted — enable weighted ECMP calculations.
**show ip flow**

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

**Syntax**

```
show ip flow interface {source-ip address destination-ip address} 
(protocol number [tcp | udp]) {src-port number destination-port number}
```

**Parameters**

`interface interface` - Enter the keyword `interface` then one of the following interface keywords.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

`source-ip address` - Enter the keywords `source-ip` then the IP source address in IP address format.

`destination-ip address` - Enter the keywords `destination-ip` then the IP destination address in IP address format.

`protocol number [tcp | udp]` - Enter the keyword `protocol` then one of the protocol type keywords: `tcp`, `udp`, or `protocol number`. The protocol number range is from 0 to 255.

`src-port number` - Enter the keywords `src-port` then the source port number.

`destination-port number` - Enter the keywords `destination-port` then the destination port number.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.9.1.0</td>
<td>Introduced VRF on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
### Version Description

7.5.1.0  Introduced on the C-Series.

pre-6.1.1.0  Introduced on the E-Series.

### Usage Information
This command provides egress port information for a given IP flow. This information is useful in identifying which interface the packet follows in the case of Port-channel and Equal Cost Multi Paths. Use this command for routed packed only. For switched packets, use the `show port-channel-flow` command.

The `show ip flow` command does not compute the egress port information when `load-balance mac hashing` is also configured due to insufficient information (the egress MAC is not available).

S-Series produces the following error message: %Error: Unable to read IP route table.

### Example

Dell# show ip flow interface Gi 2/42 20.1.1.1 100.1.1.2 protocol tcp
Flow: 20.1.1.1 100.1.1.2 6
Ingress interface: Gi 2/42
Egress Interface: Gi 2/43
Dell#

### show ip interface

View IP-related information on all interfaces.

#### Syntax

```
show ip interface [interface | brief] [configured]
```

#### Parameters

- **interface**
  
  (OPTIONAL)
  
  Enter the following keywords and the interface information:
  
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For the Management interface on the stack-unit, enter the keyword ManagementEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a Null interface, enter the keyword null then the Null interface number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.
  - For a stack-unit interface, enter the keyword stack-unit then the stack unit number.
  - For a tunnel interface, enter the keyword tunnel then the tunnel interface number. The range is from 1 to 16383.

- **brief**
  
  (OPTIONAL) Enter the keyword brief to view a brief summary of the interfaces and whether an IP address is assigned.
configured (OPTIONAL) Enter the keyword configured to display the physical interfaces with non-default configurations only.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.2</td>
<td>Supported on the E-Series E600i.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show ip interface command shown in the following example.

<table>
<thead>
<tr>
<th>Lines</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TenGigabitEthernet 1/1</td>
<td>Displays the interface’s type, physical and line protocol status.</td>
</tr>
<tr>
<td>Internet address...</td>
<td>States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.</td>
</tr>
<tr>
<td>IP MTU is...</td>
<td>Displays IP MTU value.</td>
</tr>
<tr>
<td>Inbound access...</td>
<td>Displays the name of the configured incoming access list. If none is configured, the phrase “not set” is displayed.</td>
</tr>
<tr>
<td>Proxy ARP...</td>
<td>States whether proxy ARP is enabled on the interface.</td>
</tr>
<tr>
<td>Split horizon...</td>
<td>States whether split horizon for RIP is enabled on the interface.</td>
</tr>
<tr>
<td>Poison Reverse...</td>
<td>States whether poison for RIP is enabled on the interface.</td>
</tr>
<tr>
<td>ICMP redirects...</td>
<td>States if ICMP redirects are sent.</td>
</tr>
<tr>
<td>ICMP unreachable...</td>
<td>States if ICMP unreachable messages are sent.</td>
</tr>
</tbody>
</table>
Example

Dell# show ip int gi 1/1
GigabitEthernet 1/1 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
Dell#

Usage Information

The following describes the show ip interface brief command shown in the following example.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays type of interface and the associated slot and port number.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>Displays the IP address for the interface, if configured.</td>
</tr>
<tr>
<td>Ok?</td>
<td>Indicates if the hardware is functioning properly.</td>
</tr>
<tr>
<td>Method</td>
<td>Displays “Manual” if the configuration is read from the saved configuration.</td>
</tr>
<tr>
<td>Status</td>
<td>States whether the interface is enabled (up) or disabled (administratively down).</td>
</tr>
<tr>
<td>Protocol</td>
<td>States whether IP is enabled (up) or disabled (down) on the interface.</td>
</tr>
</tbody>
</table>

Example (Brief)

Dell# show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet 1/1 unassigned NO Manual administratively down down
GigabitEthernet 1/2 unassigned NO Manual administratively down down
GigabitEthernet 1/3 unassigned YES Manual up up
GigabitEthernet 1/4 unassigned YES Manual up up
GigabitEthernet 1/5 unassigned YES Manual up up
GigabitEthernet 1/6 10.10.10.1 YES Manual up up
GigabitEthernet 1/7 unassigned NO Manual administratively down down

show ip management-route

View the IP addresses assigned to the Management interface.

Syntax

show ip management-route [all | connected | summary | static]

Parameters

- all (OPTIONAL) Enter the keyword 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
show ipv6 management-route

Display the IPv6 static routes configured for the management interface.

Syntax

```
show ipv6 management-route [all | connected | summary | static]
```

Parameters

- **all** (OPTIONAL) Enter the keyword all to view all IP addresses assigned to all Management interfaces on the switch.
- **connected** (OPTIONAL) Enter the keyword connected to view only routes directly connected to the Management interface.
- **summary** (OPTIONAL) Enter the keyword summary to view a table listing the number of active and non-active routes and their sources.
- **static** (OPTIONAL) Enter the keyword static to view non-active routes also.

Command Modes

EXEC Privilege
show ip protocols

View information on all routing protocols enabled and active on the switch.

Syntax

```
show ip protocols
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version  Description
9.8(10)   Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)  Introduced on the S6000-ON.
9.2(1.0)  Introduced on the Z9500.
9.0.2.0   Introduced on the S6000.
9.0.0.0   Introduced on the Z9000.
8.3.7.0   Introduced on the S4810.
8.3.19.0  Introduced on the S4820T.
8.4.1.0   Introduced on the C- and E-Series.
8.3.19.0  Introduced on the S4820T.
```

Example

```
show ipv6 management-route
IPv6 Destination   Gateway                 State
----------------    -------                -----  
2001:34::0/64      ManagementEthernet 1/1  Connected  
2001:68::0/64      2001:34::16             Active  
Dell#
```

IPv4 Routing

IPv4 Routing
**Version** | **Description**
---|---
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.6.1.0 | Regular evaluation optimization enabled/disabled added to display output.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.0 | Introduced on the E-Series.

**Example**

```
Dell# show ip protocols
Routing Protocol is "bgp 1"
   Cluster Id is set to 20.20.20.3
   Router Id is set to 20.20.20.3
   Fast-external-fallover enabled
   Regular expression evaluation optimization enabled
   Capable of ROUTE REFRESH
   For Address Family IPv4 Unicast
   BGP table version is 0, main routing table version 0
   Distance: external 20 internal 200 local 200
   Neighbor(s):
      Address : 20.20.20.2
      Filter-list in : foo
      Route-map in : foo
      Weight : 0
      Address : 5::6
      Weight : 0
Dell#
```

**show ip route**

View information, including how they were learned, about the IP routes on the switch.

**Syntax**

```
show ip route [vrf vrf-name] hostname | ip-address [mask] [longer-prefixes] | list prefix-list | protocol [process-id | routing-tag] | all | connected | static | summary]
```

**Parameters**

- `vrf vrf-name` *(OPTIONAL)* Enter the keyword vrf and then the VRF name to list the routes in the route table of a specific VRF.
- `ip-address` *(OPTIONAL)* Specify a name of a device or the IP address of the device to view more detailed information about the route.
- `mask` *(OPTIONAL)* Specify the network mask of the route. Use this parameter with the IP address parameter.
- `longer-prefixes` *(OPTIONAL)* Enter the keywords longer-prefixes to view all routes with a common prefix.
- `list prefix-list` *(OPTIONAL)* Enter the keyword list and the name of a configured prefix list. For more information, refer to the `show ip route list` command.
protocol

(Optional) Enter the name of a routing protocol (bgp, isis, ospf, rip) or the keywords connected or static.

NOTE: bgp, isis, ospf, and rip.

- If you enter bgp, you can include the BGP as-number.
- If you enter isis, you can include the ISIS routing-tag.
- If you enter ospf, you can include the OSPF process-id.

process-id

(Optional) Specify that only OSPF routes with a certain process ID must be displayed.

routing-tag

(Optional) Specify that only ISIS routes with a certain routing tag must be displayed.

connected

(Optional) Enter the keyword connected to view only the directly connected routes.

all

(Optional) Enter the keyword all to view both active and non-active routes.

static

(Optional) Enter the keyword static to view only routes the ip route command configures.

summary

(Optional) Enter the keyword summary. For more information, refer to the show ip route summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(2.0) Introduced on the S3100 series.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.4.(0.0) Added support for VRF.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.9.1.0 Introduced VRF on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

Usage Information

The following describes the show ip route all command in the following example.
Field | Description
--- | ---
(undefined) | Identifies the type of route:
- C = connected
- S = static
- R = RIP
- B = BGP
- IN = internal BGP
- EX = external BGP
- LO = Locally Originated
- O = OSPF
- IA = OSPF inter area
- N1 = OSPF NSSA external type 1
- N2 = OSPF NSSA external type 2
- E1 = OSPF external type 1
- E2 = OSPF external type 2
- i = IS-IS
- L1 = IS-IS level-1
- L2 = IS-IS level-2
- IA = IS-IS inter-area
- * = candidate default
- > = non-active route
- + = summary routes

The weight for weighted ECMP route calculations is displayed for each path in the route in `show ip route` command. The ECMP weight is displayed only if weighted ECMP is enabled using the `ip ecmp weighted` command is enabled.

If weighted ECMP is disabled, the `show ip route` command does not show the weighted ECMP route information.

Destination | Identifies the route’s destination IP address
Gateway | Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric | Identifies if the route has a specified distance or metric.
Last Change | Identifies when the route was last changed or configured.

Example

Dell# show ip route all

Codes:C- connected, S - static, R - RIP
B- BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated
O- OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
L2 - IS-IS level-2, IA - IS-IS inter-area, * - candidate default
> - non-active route + - summary route

Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0.0.0/8</td>
<td>via 100.10.10.10, Gi 2/8</td>
<td>120/1</td>
<td>00:07:12</td>
</tr>
<tr>
<td>100.10.10.0/24</td>
<td>Direct, Gi 2/8</td>
<td>0/0</td>
<td>00:08:54</td>
</tr>
<tr>
<td>&gt; R 100.10.10.0/24</td>
<td>Direct, Gi 2/8</td>
<td>120/0</td>
<td>00:08:54</td>
</tr>
</tbody>
</table>
Example (Summary)

Dell# show ip route summary

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Active Routes</th>
<th>Non-active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>static</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total 3 active route(s) using 612 bytes

R1_E600i# show ip route static?
<table>
<thead>
<tr>
<th>Pipe through a command</th>
</tr>
</thead>
</table>

R1_E600i# show ip route static

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>via 10.10.91.9, Gi 1/2</td>
<td>1/0</td>
<td>3d2h</td>
</tr>
</tbody>
</table>

Example (vrf)

Dell# show ip route vrf test1

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.0.0.0/24</td>
<td>Direct, Gi 1/17</td>
<td>0/0</td>
<td>00:00:04</td>
</tr>
</tbody>
</table>

Example (With Weighted ECMP Enabled)

Dell(conf)# ip route 1.1.1.0/24 6.6.6.2 weight 100
Dell(conf)# ip route 1.1.1.0/24 6.6.6.2 weight 200

Dell(conf)# show ip route

Codes: C - connected, S - static, R - RIP,
B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
> - non-active route, + - summary route

Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>4.4.4.2, via Gi 1/4, weight 100</td>
<td>1/0</td>
<td>00:00:01</td>
</tr>
<tr>
<td></td>
<td>6.6.6.2, via Gi 1/16, weight 200</td>
<td>0/0</td>
<td>00:01:32</td>
</tr>
</tbody>
</table>

Dell# show ip route 1.1.1.0/24

Routing entry for 1.1.1.0/24
Known via "static", distance 1, metric 0
Last update 00:05:01 ago
Routing Descriptor Blocks:
* 4.4.4.2, via GigabitEthernet 1/4 weight 100
  * 6.6.6.2, via GigabitEthernet 1/16 weight 200

Dell(conf)#

Example (With Weighted ECMP Disabled)

Dell(conf)# ip route 1.1.1.0/24 6.6.6.2 weight 100
Dell(conf)# ip route 1.1.1.0/24 6.6.6.2 weight 200

Dell(conf)# show ip route

Codes: C - connected, S - static, R - RIP,
B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,
O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
> - non-active route, + - summary route

Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td>Direct, Gi 1/4</td>
<td>0/0</td>
<td>00:00:04</td>
</tr>
<tr>
<td></td>
<td>Direct, Gi 1/16</td>
<td>0/0</td>
<td>00:01:32</td>
</tr>
</tbody>
</table>
show ip route list

Display IP routes in an IP prefix list.

Syntax

show ip route [vrf vrf-name] list prefix-list

Parameters

prefix-list Enter the name of a configured prefix list.

vrf vrf-name Enter the keyword vrf followed by the name of the VRF to display IP routes in an IP prefix list corresponding to that VRF.

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(10) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048–ON.
9.8(0.0P2) Introduced on the S3048–ON.
9.7(0.0) Introduced on the S6000–ON.
9.4(0.0) Added support for VRF.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3(19.0) Introduced on the S4820T.
8.3(11.1) Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.1.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.
Example

```
Dell# show ip route list test

Codes: C- connected, S - static, R - RIP, B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated, O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type 1, E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1, L2- IS-IS level-2, IA - IS-IS inter area, * - candidate default, >- non-active route, + - summary route

Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Dist/Metric</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>R 2.1.0.0/24</td>
<td>via 2.1.4.1, Gi 4/43</td>
<td>120/2</td>
<td>3d0h</td>
</tr>
<tr>
<td>R 2.1.1.0/24</td>
<td>via 2.1.4.1, Gi 4/43</td>
<td>120/2</td>
<td>3d1h</td>
</tr>
<tr>
<td>R 2.1.2.0/24</td>
<td>via 2.1.4.1, Gi 4/43</td>
<td>120/1</td>
<td>3d1h</td>
</tr>
<tr>
<td>R 2.1.3.0/24</td>
<td>via 2.1.4.1, Gi 4/43</td>
<td>120/1</td>
<td>3d1h</td>
</tr>
<tr>
<td>C 2.1.4.0/24</td>
<td>Direct, Gi 4/43</td>
<td>0/0</td>
<td>3d1h</td>
</tr>
</tbody>
</table>
```

Related Commands

- `ip prefix-list` — enter CONFIGURATION-IP PREFIX-LIST mode and configures a prefix list.
- `show ip prefix-list summary` — display a summary of the configured prefix lists.

**show ip route summary**

View a table summarizing the IP routes in the switch.

**Syntax**

```
show ip route [vrf vrf-name] [summary]
```

**Parameters**

- `vrf vrf-name` Enter the keyword vrf followed by the name of the VRF to view information on the IP routes corresponding to that VRF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(0.2)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
### Version Description
- **8.3.11.1**: Introduced on the Z9000.
- **8.3.7.0**: Introduced on the S4810.
- **8.1.1.0**: Introduced on the E-Series.
- **7.6.1.0**: Introduced on the S-Series.
- **7.5.1.0**: Introduced on the C-Series.
- **pre-6.1.1.0**: Introduced on the E-Series.

### Usage Information
The following describes the `show ip route summary` shown in the following example.

#### Column Heading Description
- **Route Source**: Identifies how the route is configured in Dell Networking OS.
- **Active Routes**: Identifies the best route if a route is learned from two protocol sources.
- **Non-active Routes**: Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route becomes the best route.
- **ospf 100**: If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
- **Total 1388 active...**: Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the Dell Networking OS, this line does not appear.

### Example
```
Dell> show ip route summary

Route Source  Active Routes  Non-active Routes
connected      17            0
static         3             0
ospf 100       1368          2
Intra-area: 762  Inter-area: 1  External-1: 600  External-2: 5
Total          1388         2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Dell>
```

### Related Commands
- `show ip route` — display information about the routes found in the switch.

### show ip traffic
View IP, ICMP, UDP, TCP and ARP traffic statistics.

#### Syntax
```
show ip traffic [all | cp | rp1 | rp2]
```

| NOTE: These options are supported only on the E-Series.

#### Parameters
- **all** (OPTIONAL) Enter the keyword all to view statistics from all processors. If you do not enter a keyword, you also view all statistics from all processors.
cp (OPTIONAL) Enter the keyword cp to view only statistics from the Control Processor.

rp1 (OPTIONAL) Enter the keyword rp1 to view only the statistics from Route Processor 1.

rp2 (OPTIONAL) Enter the keyword rp2 to view only the statistics from Route Processor 2.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>F10 Monitoring MIB available for the ip traffic statistics command.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The following describes the show ip traffic summary shown in the following example.

Keyword | Definition
unknown protocol... | No receiver for these packets. Counts packets whose protocol type field is not recognized by Dell Networking OS.
not a gateway... | Packets can not be routed; the host/network is unreachable.
security failures... | Counts the number of received unicast/multicast packets that could not be forwarded due to:
bad options... | Unrecognized IP option on a received packet.
Frags: | IP fragments received.
... reassembled | Number of IP fragments that were reassembled.
... timeouts | Number of times a timer expired on a reassembled queue.
... too big | Number of invalid IP fragments received.
... couldn't fragment | Number of packets that could not be fragmented and forwarded.
Keyword     Definition
encapsulation failed     Counts packets which could not be forwarded due to ARP resolution failure. Dell Networking OS sends an ARP request prior to forwarding an IP packet. If a reply is not received, Dell Networking OS repeats the request three times. These packets are counted in encapsulation failed.

Rcvd:
short packets     The number of bytes in the packet are too small.
bad length     The length of the packet was not correct.
no port broadcasts     The incoming broadcast/multicast packet did not have any listener.
socket full     The applications buffer is full and the incoming packet are dropped.

The Dell Monitoring MIB provides access to the following statistics.

- **IP Statistics: Bcast: Received**: Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent**: Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received**: Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent**: Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request**: Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies**: Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request**: Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies**: Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy**: Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

**Example**

```
Dell# show ip traffic
Control Processor IP Traffic:

IP statistics:
  Rcvd: 23857 total, 23829 local destination
    0 format errors, 0 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    0 security failures, 0 bad options
    0 reassembled, 0 timeouts, 0 too big
    0 fragmented, 0 couldn't fragment
  Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
  Sent: 16048 generated, 0 forwarded
    21 encapsulation failed, 0 no route

ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
    0 parameter, 0 timestamp, 0 info request, 0 other
    Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem

UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
    0 short packets, 0 bad length, 0 no port broadcasts, 0 socket full
  Sent: 0 total, 0 forwarded broadcasts

TCP statistics:
  Rcvd: 23829 total, 0 checksum errors, 0 no port
  Sent: 16048 total

ARP statistics:
  Rcvd: 156 requests, 11 replies
  Sent: 21 requests, 10 replies (0 proxy)
Routing Processor1 IP Traffic:
```
show tcp statistics

View information on TCP traffic through the switch.

Syntax

```
show tcp statistics {all | cp}
```

Parameters

- **all**: Enter the keyword all to view all TCP information.
- **cp**: Enter the keyword cp to view only TCP information from the Control Processor.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>6.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the `show tcp statistics cp` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvd:</td>
<td>Displays the number and types of TCP packets received by the switch.</td>
</tr>
<tr>
<td>0 checksum error...</td>
<td>Displays the number of packets received with the following:</td>
</tr>
<tr>
<td>329 packets...</td>
<td>Displays the number of packets and bytes received in sequence.</td>
</tr>
<tr>
<td>17 dup...</td>
<td>Displays the number of duplicate packets and bytes received.</td>
</tr>
<tr>
<td>0 partially...</td>
<td>Displays the number of partially duplicated packets and bytes received.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 out-of-order...</td>
<td>Displays the number of packets and bytes received out of order.</td>
</tr>
<tr>
<td>0 packets with data after window</td>
<td>Displays the number of packets and bytes received that exceed the switch’s window size.</td>
</tr>
<tr>
<td>0 packets after close</td>
<td>Displays the number of packet received after the TCP connection was closed.</td>
</tr>
<tr>
<td>0 window probe packets...</td>
<td>Displays the number of window probe and update packets received.</td>
</tr>
<tr>
<td>41 dup ack...</td>
<td>Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.</td>
</tr>
<tr>
<td>10184 ack...</td>
<td>Displays the number of acknowledgement packets and bytes received.</td>
</tr>
<tr>
<td>Sent:</td>
<td>Displays the total number of TCP packets sent and the number of urgent packets sent.</td>
</tr>
<tr>
<td>25 control packets...</td>
<td>Displays the number of control packets sent and the number retransmitted.</td>
</tr>
<tr>
<td>11603 data packets...</td>
<td>Displays the number of data packets sent.</td>
</tr>
<tr>
<td>24 data packets retransmitted</td>
<td>Displays the number of data packets resent.</td>
</tr>
<tr>
<td>355 ack...</td>
<td>Displays the number of acknowledgement packets sent and the number of packet delayed.</td>
</tr>
<tr>
<td>0 window probe packets...</td>
<td>Displays the number of window probe and update packets sent.</td>
</tr>
<tr>
<td>7 Connections initiated...</td>
<td>Displays the number of TCP connections initiated, accepted, and established.</td>
</tr>
<tr>
<td>14 Connections closed...</td>
<td>Displays the number of TCP connections closed, dropped.</td>
</tr>
<tr>
<td>20 Total rxmt...</td>
<td>Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.</td>
</tr>
<tr>
<td>0 Keepalive....</td>
<td>Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.</td>
</tr>
</tbody>
</table>

### Example

Dell# show tcp stat cp

```
Control Processor TCP:
Rcvd: 10585 Total, 0 no port
  0 checksum error, 0 bad offset, 0 too short
  329 packets (1263 bytes) in sequence
  17 dup packets (6 bytes)
  0 partially dup packets (0 bytes)
  7 out-of-order packets (0 bytes)
  0 packets ( 0 bytes) with data after window
  0 packets after close
  0 window probe packets, 41 window update packets
  41 dup ack packets, 0 ack packets with unsend data
  10184 ack packets (12439508 bytes)
Sent: 12007 Total, 0 urgent packets
  25 control packets (including 24 retransmitted)
  11603 data packets (12439677 bytes)
  24 data packets (7638 bytes) retransmitted
  355 ack only packets (41 delayed)
  0 window probe packets, 0 window update packets
  7 Connections initiated, 8 connections accepted, 15 connections established
  14 Connections closed (including 0 dropped, 0 embryonic dropped)
  20 Total rxmt timeout, 0 connections dropped in rxmt timeout
  0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```
IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking OS.

**NOTE:** For IPv4 ACL commands, see Access Control Lists (ACL).

### Important Points to Remember

- Certain platforms require manual CAM usage space allotment. For more information, see `cam-acl`.
- 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:

- `show cam-acl-egress`
- `show cam-acl`
- `permit icmp`
- `permit`
- `ipv6 control-plane egress-filter`
- `ipv6 access-list`
- `cam-acl-egress`
- `cam-acl`

### show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

**Syntax**

```
show cam-acl-egress
```

**Command Modes**

- EXEC
- EXEC Privilege
show cam-acl

Show space allocated for IPv6 ACLs.

Syntax

show cam-acl

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
show cam-acl (non default)
Dell(conf)# cam-acl l2acl 2 ipv4acl 4 ipv6acl 4 ipv4qos 2 l2qos 1 l2pt 0
ipmacacl 0 vman-qos 0 ecfmacl 0
Dell#show cam-acl

-- Chassis Cam ACL --
Current Settings(in block sizes)
  1 block = 128 entries
L2Acl        :         2
Ipv4Acl      :         4
Ipv6Acl      :         4
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
FcoeAcl      :         0
iscsiOptAcl  :         0
ipv4pbr      :         0
vrfv4Acl     :         0
Openflow     :         0
fedgovacl    :         F3940

-- stack-unit 1 --
Current Settings(in block sizes)
  1 block = 128 entries
L2Acl        :         2
Ipv4Acl      :         4
Ipv6Acl      :         4
Ipv4Qos      :         2
L2Qos        :         1
L2PT         :         0+F394
IpMacAcl     :         0
VmanQos      :         0
VmanDualQos  :         0
EcfmAcl      :         0
FcoeAcl      :         0
iscsiOptAcl  :         0
ipv4pbr      :         0
vrfv4Acl     :         0
Openflow     :         0
fedgovacl    :         0
Dell#
```
Example (Manual Profiles)

Dell# show cam-acl

-- Chassis Cam ACL --
  Current Settings(in block sizes)
  L2Acl   :         2
  Ipv4Acl :         2
  Ipv6Acl :         4
  Ipv4Qos :         2
  L2Qos   :         3

-- Line card 4 --
  Current Settings(in block sizes)
  L2Acl   :         2
  Ipv4Acl :         2
  Ipv6Acl :         4
  Ipv4Qos :         2
  L2Qos   :         3

Dell#

Related Commands
  •  cam-acl — configure CAM profiles to support IPv6 ACLs.

permit icmp

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax
  permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] | [log] [monitor]

To remove this filter, you have two choices:
  •  Use the no seq sequence-number command if you know the filter's sequence number.
  •  Use the no permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} command.

Parameters

Defaults
  Not configured.

Command Modes
  ACCESS-LIST

Command History
  This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series. Added the monitor option.</td>
</tr>
</tbody>
</table>

**permit**

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

**Syntax**

```
permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

**Parameters**

- `ipv6-protocol-number` Enter an IPv6 protocol number. The range is from 0 to 255.
- `icmp` Enter the keyword `icmp` to filter internet Control Message Protocol version 6.
- `ipv6` Enter the keyword `ipv6` to filter any internet Protocol version 6.
- `tcp` Enter the keyword `tcp` to filter the Transmission Control protocol.
- `udp` Enter the keyword `udp` to filter the User Datagram Protocol.

**Defaults**

Not configured.

**Command Modes**

ACCESS-LIST

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

Syntax
ipv6 control-plane egress-filter

Defaults Not enabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Syntax
ipv6 access-list access-list-name cpu-qos

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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for CoPP for OSPFV3 on the S4810, S4820T, S6000, and Z9000 platforms.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series. Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation. You can create an IPv6 ACL for control-plane traffic policing for OSPFV3, in addition to the CoPP support for VRRP, BGP, and ICMP.

cam-acl-egress
Allocate space for IPv6 egress ACLs.

Syntax
cam-acl-egress {default | l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}

Parameters
- `default` Use the default CAM profile settings, and set the CAM as follows:
  - L2 ACL(l2acl): 1
  - L3 ACL (ipv4acl): 1
  - IPv6 L3 ACL (ipv6acl): 2
Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 4. The ipv6acl range must be a factor of 2.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

For the new settings to take effect, save the new CAM settings to the startup-config (write-mem or copy run start), then reload the system.

The total amount of space allowed is 4 FP Blocks.

**Example**

```
Dell(conf)# 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 2
```

IPv6 Access Control Lists (IPv6 ACLs)
Allocate space for IPv6 ACLs.

Syntax

```plaintext
cam-acl {default | l2acl l-10 ipv4acl l-10 ipv6acl 0-10 ipv4qos l-10 l2qos l-10}
```

Parameters

- **default**: Use the default CAM profile settings, and set the CAM as follows:
  - L3 ACL (ipv4acl): 6
  - L2 ACL(l2acl): 5
  - IPv6 L3 ACL (ipv6acl): 0
  - L3 QoS (ipv4qos): 1
  - L2 QoS (l2qos): 1

- **l2acl l-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos 1-10**: Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The ipv6acl range must be a factor of 2.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7(0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(2.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (write-mem or copy run start), then reload the system.
The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 13.

Ranges for the CAM profiles are from 1 to 10, except for the ipv6acl profile which is from 0 to 10. The ipv6acl allocation must be a factor of 2 (2, 4, 6, 8, 10).
IPv6 Basics

IPv6 basic commands are supported on the Dell Networking OS.

NOTE: For information about the Dell Networking OS version and platform that supports IPv6 in each software feature, see the IPv6 Addressing section in the Dell Networking OS Configuration Guide.

Topics:
- clear ipv6 fib
- clear ipv6 route
- clear ipv6 mld_host
- maximum dynamic-routes-ipv6
- 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 dns-server
- ipv6 nd prefix
- 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 stack unit.

Syntax:
```
clear ipv6 fib [vrf vrf-name] stack-unit unit-number
```
clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

Syntax

```plaintext
clear ipv6 route [vrf vrf-name] {*} | ipv6-address prefix-length
```

Parameters

- **vrf vrf-name** (Optional) Enter the keyword vrf followed by the name of the VRF to clear the IPv6 routes corresponding to that VRF.
- *** | ipv6-address prefix-length** 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 format then the prefix length in the /x format. The range is from /0 to /128.

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.2(1.0)  Introduced on the Z9500.
- 9.0.0.0  Introduced on the Z9000.
- 8.3.19.0  Introduced on the S4820T.
- 8.3.7.0  Introduced on the S4810.
- 8.2.1.0  Introduced on the E-Series.
- 7.8.1.0  Introduced on the C-Series and S-Series.
- 7.4.1.0  Introduced on the E-Series.

**clear ipv6 route**

Clear (refresh) all or a specific route from the IPv6 routing table.

**Syntax**

```plaintext
clear ipv6 route [vrf vrf-name] {*} | ipv6-address prefix-length
```

**Parameters**

- **vrf vrf-name** (Optional) Enter the keyword vrf followed by the name of the VRF to clear the IPv6 routes corresponding to that VRF.
- *** | ipv6-address prefix-length** 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 format then the prefix length in the /x format. The range is from /0 to /128.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

Syntax

```
clear ipv6 mld_host
```

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

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.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on the E-Series.
7.8.1.0 Introduced on the C-Series and S-Series.
7.4.1.0 Introduced on the E-Series.

maximum dynamic-routes-ipv6

Specify the maximum number of dynamic (protocol) IPv6 routes a VRF can have.

Syntax

```
maximum dynamic-routes-ipv6 limit \{warn-threshold threshold-value | warning-only\}
```

Example

```
Dell(conf)
```

Dell(conf)

**Related Commands**

- clear ipv6 mld_host
- show ipv6 mld_host
To remove the limit on the maximum number of IPv6 routes used, use the `no maximum dynamic-routes-ipv6` command.

**Parameters**

- **limit**: Maximum number of IPv6 routes allowed in a VRF. Valid range is from 1 to 8000 (or maximum allowable for that platform if smaller value).
- **warning-threshold**: Warning threshold value is expressed as a percentage of the limit value. When the number of IPv6 routes reaches the specified percentage of the limit, a warning message is generated. Valid range is 1 to 100. When warn-threshold is used, once the limit is reached, additional routes will not be allowed into the RTM (route table manager) itself.
- **warning-only**: When the warning-only option is used, a syslog message will be thrown when maximum number of dynamic IPv6 routes reaches the limit. Additional dynamic IPv6 routes will still be allowed.

**Defaults**

No limit is set on the maximum number of dynamic IPv6 routes for a VRF.

**Command Modes**

`CONFIGURATION-VRF`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.</td>
</tr>
</tbody>
</table>

**Usage Information**

If the maximum IPv6 route limit is not specified for a VRF (valid range is from 1 to 8000), then it has unlimited space that extends to the maximum number of entries allowed for the system. This command is not applicable to the default and management VRFs.

**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)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**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** prefix-length
  Enter the IPv6 address in the `x:x:x:x:x` format then the prefix length in the `/x` format. The range is from `/0` to `/128`.

- **NOTE:** The `::` notation specifies successive hexadecimal fields of zeros.

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.1.(0.0) | Updated Usage Information section.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.

**Usage 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 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**

- `ipv6-address prefix-length` Enter the IPv6 prefix in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.
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}
```

Parameters

- **pps**
  - 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`

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

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 gig 1/4
Dell(conf-if-gi-1/4)# ipv6 address 200:1::/64 eui64
Dell(conf)# int gig 1/6
Dell(conf-if-gi-1/6)# ipv6 address 801:10::/64 eui64
```
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 protocol operations to fill the field, use the no ipv6 flowlabel-zero command.

Default
Disabled

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.

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::X) to be mapped to the name.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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::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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.4.2.1 | Introduced on the C-Series and S-Series.
8.4.1.0 | Introduced on the E-Series.

**Usage Information**

You can separately configure both IPv4 and IPv6 domain name servers.

In a dual stack setup, the system sends both A (request for IPv4 — RFC 1035) and AAAA (request for IPv6 — RFC 3596) record requests to a DNS server even if only the `ip name-server` command is configured.

### ipv6 nd dad attempts

To perform duplicate address detection (DAD) on an 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)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### ipv6 nd dns-server

Configures Recursive DNS Server (RDNSS) addresses to be distributed via IPv6 router advertisements to an IPv6 device.

**Syntax**

```
ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}
```

To remove the IPv6 RDSS configuration, use `no ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}`.
Parameters

ipv6-RDNSS-address
Enter the IPv6 Recursive DNS Server’s (RDNSS) address. You can specify up to 4 IPv6 RDNSS server addresses.

lifetime
Enter the lifetime in seconds. The amount of time the IPv6 host can use the IPv6 RDNSS address for name resolution. The range is 0 to 4294967295 seconds. When you specify the maximum lifetime value of 4294967295 or infinite, the lifetime does not expire. A value of 0 indicates to the host that the RDNSS address should not be used. You must specify a lifetime using the lifetime or infinite parameter.

infinite
Enter the keyword infinite to specify that the RDNSS lifetime does not expire.

Defaults
Not Configured

Command Modes INTERFACE CONFIG

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.5(0.0) Introduced on the Z9000, S6000, S4810, S4820T, and MXL..

Usage Information
Use this command to add, edit, or delete an IPv6 RDNSS address and lifetime value. You can configure up to four IPv6 RDNSS addresses. You must specify a lifetime using the lifetime or infinite parameter.

Example
Dell(conf-if-gi-1/1)# ipv6 nd dns-server 1000::1 1

ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

Syntax
ipv6 nd prefix {ipv6-prefix | prefix-length | default} [no-advertise] | [no-autoconfig] [no-rtr-address] [off-link] [lifetime {valid | infinite} {preferred | infinite}]

Parameters
ipv6-prefix
Enter an IPv6 prefix.

prefix-length
Enter the prefix then the prefix length. The length range is from 0 to 128.

default
Enter the keyword default to set default parameters for all prefixes.

no-advertise
Enter the keyword no-advertise to prevent the specified prefix from being advertised.

no-autoconfig
Enter the keywords no-autoconfig to disable Stateless Address Autoconfiguration.

no-rtr-address
Enter the keyword no-rtr-address to exclude the full router address from router advertisements (the R bit is not set).
off-link Enter the keywords off-link to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.

valid-lifetime | infinite Enter the amount of time that the prefix is advertised, or enter infinite for an unlimited amount of time. The range is from 0 to 4294967295. The default is 2592000. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.

preferred-lifetime | infinite Enter the amount of time that the prefix is preferred, or enter infinite for an unlimited amount of time. The range is from 0 to 4294967295. The default is 604800. The maximum value means that the preferred lifetime and does not expire.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.3.2.0 Introduced on the E-Series, C-Series, and S-Series.

Usage Information By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the default keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the ipv6 nd prefix default no-autoconfig command.

ipv6 route

Establish a static IPv6 route.

Syntax
ipv6 route [vrf vrf-name] ipv6-address prefix-length [ipv6-address | interface | interface ipv6-address] [distance] [tag value] [permanent] [weight weight-value]

To remove the IPv6 route, use the no ipv6 route command.

Parameters
vrf vrf-name (Optional) Enter the keyword vrf followed by the name of the VRF to install IPv6 routes in that VRF.

ipv6-address prefix-length Enter the IPv6 address in the 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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a 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::x format.

**distance**

(Optional) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.

**tag**

(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.

**weight**

Enter the keyword weight followed by a weight value. The range is from 0 to 255.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Also included the weight parameter to support weighted ECMP feature. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### Version Description

- **9.0.0.0**: Introduced on the Z9000.
- **8.3.19.0**: Introduced on the S4820T.
- **8.3.7.0**: Introduced on the S4810.
- **8.5.1.0**: Added support for 4-port 40G line cards on the E-Series.
- **8.2.1.0**: Introduced on the E-Series.
- **7.8.1.0**: Introduced on the C-Series and S-Series.
- **7.4.1.0**: Introduced on the E-Series.

### Usage Information

When the interface goes down, Dell Networking OS withdraws the route. The route is re-installed, by Dell Networking OS, when the interface comes back up. When a recursive resolution is “broken,” Dell Networking OS withdraws the route. The route is re-installed, by Dell Networking OS, when the recursive resolution is satisfied.

After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.

You can specify a weight for an IPv4 or IPv6 static route. If the weight value of a path is 0, then that path is not used for forwarding when weighted ECMP is in effect. Also, if a path corresponding to a static route (destination) has a non-zero weight assigned to it and other paths do not have any weight configured, then regular ECMP is used for forwarding.

You can specify the weight value only to destination address and not on the egress port.

A route is considered for weighted ECMP calculations only if each paths corresponding to that route is configured with a weight.

### Example

```plaintext
Dell(conf)# ipv6 route 44::/64 33::1 weight 100
Dell(conf)# ipv6 route 44::/64 33::2 weight 200
Dell(conf)# do show running-config | grep ipv6 route
Dell(conf)# ipv6 route vrf vrf_test 44::/64 33::1 weight 100
Dell(conf)# ipv6 route vrf vrf_test 44::/64 33::2 weight 200
Dell(conf)# do show running-config | grep ipv6 route vrf
```

### Related Commands
- `show ipv6 route` — view the IPv6 configured routes.

### ipv6 unicast-routing

Enable IPv6 unicast routing on the device.

#### Syntax

`ipv6 unicast-routing`

To disable unicast routing, use the `no ipv6 unicast-routing` command.

#### Defaults

- **Enabled**

#### Command Modes

- **CONFIGURATION**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

## Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

## 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, Dell Networking OS generates a syslog message indicating the action. Disabling unicast routing on an E-Series chassis causes the following behavior:

- static and protocol learned routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered

### show ipv6 cam stack-unit

Displays the IPv6 CAM entries for the specified stack-unit.

#### Syntax

```
show ipv6 cam [vrf vrf-name] stack-unit unit-number port-set {0-1} [summary | index | ipv6 address]
```

#### Parameters

- **vrf vrf-name**  
  (Optional) Enter the keyword vrf followed by the name of the VRF to display IPv6 CAM entries corresponding to that VRF.

  | NOTE: If you do not specify this option, IPv6 CAM entries corresponding to the default VRF are displayed.

- **unit-number**  
  Enter the stack unit’s ID number.

- **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::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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Added support for VRF.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.7.1 Introduced on the S4810.
8.4.2.1 Introduced on the S-Series.

Usage Information

NOTE: If a route has a mask greater than 64, no output is displayed and 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 {0-1} 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.

NOTE: The self address is displayed in the neighbor portion for the show ipv6 cam stack-unit unit-number port-set command.

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
show ipv6 fib stack-unit

View all FIB entries.

Syntax

show ipv6 fib [vrf vrf-name] stack-unit unit-number [summary | ipv6-address]

Parameters

vrf vrf-name
(Optional) Enter the keyword vrf followed by the name of the VRF to display neighbors corresponding to that VRF.

slot-number
Enter the number of the stack unit.

summary
(Optional) Enter the keyword summary to view a summary of entries in IPv6 cam.

ipv6-address
Enter the IPv6 address in the x:x:x:x:x:n format to display networks that have more specific prefixes. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
### show ipv6 flowlabel-zero

Display the flow label zero setting.

**Syntax**

```
show ipv6 flowlabel-zero
```

**Default**

Disabled

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.2(1.0) Introduced on the Z9500.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.11.1 Introduced on the Z9000.
- 8.3.7.0 Introduced on the S4810.

**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 {slot | slot/port} [brief] [configured] [stack-unit id]
```

**Parameters**

- `interface` (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.

For a port channel interface, enter the keywords port-channel then a number.

For a Null interface, enter the keyword null then the Null interface number.

For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

For stacking, enter the keywords stack-unit then the stack-unit ID.

For a tunnel interface, enter the keyword tunnel then the tunnel ID.

brief
(Optional) View a summary of IPv6 interfaces.

configured
(Optional) View information on all IPv6 configured interfaces.

gigabitethernet
(Optional) View information for an IPv6 gigabitethernet interface.

managementethernet slot/port
(Optional) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).

loopback
(Optional) View information for IPv6 Loopback interfaces.

port-channel
(Optional) View information for IPv6 port channels.

tengigabitethernet
(Optional) View information for an IPv6 tengigabitethernet interface.

stack-unit id
(Optional) View information for stacking.

tunnel tunnel-id
(Optional) View information for a tunnel interface.

vlan
(Optional) View information for IPv6 VLANs.

Defaults
None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.5(0.1) Added support for IPv6 recursive DNS addresses on the Z9500.

9.2(1.0) Introduced on the Z9500.
9.2,(0.0) Added support for tunnel interface.
9.0,0.0 Introduced on the Z9000.
8.3(19.0) Introduced on the S4820T.
8.3(7.0) Introduced on the S4810.
8.5(1.0) Added support for 4-port 40G line cards on the E-Series.
8.4(2.1) Introduced on the S-Series.
8.2(1.0)Introduced on the E-Series. Added support for the managementethernet slot/port parameter.
## Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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 gigabit 1/12
GigabitEthernet 1/12 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::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 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

Dell#

### Example (Managementethernet)

Dell# show ipv6 interface management 1/1
ManagementEthernet 1/1 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
GigabitEthernet 1/2 [administratively down/down]
  fe80::201:e8ff:fea7:497e
  2002:1:2::3/96
GigabitEthernet 1/12 [up/up]
  fe80::201:e8ff:fea7:497e
  100::2/64
ManagementEthernet 1/1 [up/up]
  fe80::201:e8ff:fea7:497e
Example (tunnel)

Dell# show ipv6 interface tunnel 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
Dell#

show ipv6 mld_host

Display the IPv6 MLD host counters.

Syntax

show ipv6 mld_host

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.

Usage Information
The following describes the show ipv6 mld-host command shown in the following example.

Field Description
Valid MLD Packets The total number of packets received and sent from the last time the elapsed time was cleared.
### Field Description

**Reports**
The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.

**Leaves**
The number of Multicast leaves that have been sent.

**MLDv1 queries**
The number of MLDv1 queries that have been received.

**MLDv2 queries**
The number of MLDv2 queries that have been received.

**Malformed Packets**
The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

### Example

MLD Host Traffic Counters
Elapsed time since counters cleared: 00:28:33:52

<table>
<thead>
<tr>
<th>Field</th>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid MLD Packets</td>
<td>97962</td>
<td>18036</td>
</tr>
<tr>
<td>Reports</td>
<td>79962</td>
<td>18034</td>
</tr>
<tr>
<td>Leaves</td>
<td>----</td>
<td>0</td>
</tr>
<tr>
<td>MLDv2 Queries</td>
<td>18000</td>
<td>----</td>
</tr>
<tr>
<td>MLDv1 Queries</td>
<td>0</td>
<td>----</td>
</tr>
<tr>
<td>Errors: Malformed Packets</td>
<td>4510</td>
<td></td>
</tr>
</tbody>
</table>

### show ipv6 route

Displays the IPv6 routes.

#### Syntax

```
show ipv6 route [ipv6-address prefix-length] [vrf vrf-name] [hostname] [all] [bgp as number] [connected] [isis tag] [list prefix-list name] [ospf process-id] [rip] [static] [summary]
```

#### Parameters

- **ipv6-address prefix-length** (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

  **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

- **vrf vrf-name** (Optional) Enter the keyword vrf followed by the name of the VRF to display IPv6 routes corresponding to that VRF.

  **NOTE:** If you do not specify this option, routes corresponding to the default VRF are displayed.

- **hostname** (OPTIONAL) View information for this IPv6 routes with Host Name.

- **all** (OPTIONAL) View information for all IPv6 routes.

- **bgp** (OPTIONAL) View information for all IPv6 BGP routes.

- **connected** (OPTIONAL) View only the directly connected IPv6 routes.

- **isis** (OPTIONAL) View information for all IPv6 IS-IS routes.

- **list** (OPTIONAL) View the IPv6 prefix list.

- **ospf** (OPTIONAL) View information for all IPv6 OSPF routes.
rip (OPTIONAL for E-Series only) View information for all IPv6 RIP routes.
static (OPTIONAL) View only routes configured by the ipv6 route command.
summary (OPTIONAL) View a brief list of the configured IPv6 routes.

Defaults
none

Command Modes
• EXEC
• EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The following describes the show ipv6 route command shown in the following examples.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(undefined)</td>
<td>Identifies the type of route:</td>
</tr>
<tr>
<td>• L = Local</td>
<td></td>
</tr>
<tr>
<td>• C = connected</td>
<td></td>
</tr>
<tr>
<td>• S = static</td>
<td></td>
</tr>
<tr>
<td>• R = RIP</td>
<td></td>
</tr>
<tr>
<td>• B = BGP</td>
<td></td>
</tr>
<tr>
<td>• IN = internal BGP</td>
<td></td>
</tr>
<tr>
<td>• EX = external BGP</td>
<td></td>
</tr>
<tr>
<td>• LO = Locally Originated</td>
<td></td>
</tr>
<tr>
<td>• O = OSPF</td>
<td></td>
</tr>
<tr>
<td>• IA = OSPF inter-area</td>
<td></td>
</tr>
<tr>
<td>• N1 = OSPF NSSA external type 1</td>
<td></td>
</tr>
<tr>
<td>• N2 = OSPF NSSA external type 2</td>
<td></td>
</tr>
<tr>
<td>• E1 = OSPF external type 1</td>
<td></td>
</tr>
<tr>
<td>• E2 = OSPF external type 2</td>
<td></td>
</tr>
<tr>
<td>• i = IS-IS</td>
<td></td>
</tr>
<tr>
<td>• L1 = IS-IS level-1</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>•</td>
<td>L2 = IS-IS level-2</td>
</tr>
<tr>
<td>•</td>
<td>IA = IS-IS inter-area</td>
</tr>
<tr>
<td>•</td>
<td>* = candidate default</td>
</tr>
<tr>
<td>•</td>
<td>&gt; = non-active route</td>
</tr>
<tr>
<td>•</td>
<td>+ = summary routes</td>
</tr>
</tbody>
</table>

**Destination**
Identifies the route's destination IPv6 address.

**Gateway**
Identifies whether the route is directly connected and on which interface the route is configured.

**Dist/Metric**
Identifies if the route has a specified distance or metric.

**Last Change**
Identifies when the route was last changed or configured.

### Example (S-Series)

Dell# show ipv6 route

```
Codes: C - connected, L - local, S - static, R - RIP,
       B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated,
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,

Gateway of last resort is not set

<table>
<thead>
<tr>
<th>Destination</th>
<th>Dist/Metric, Gateway, Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>C 100::/64</td>
<td>[0/0] Direct, Gi 1/12, 20:00:18</td>
</tr>
<tr>
<td>C 400::/64</td>
<td>[0/0] Direct, Tu 1, 00:09:02</td>
</tr>
<tr>
<td>S 800::/64</td>
<td>[1/0] via 100::1, Gi 1/12, 00:00:50</td>
</tr>
<tr>
<td>L fe80::/10</td>
<td>[0/0] Direct, Nu 0, 20:00:18</td>
</tr>
</tbody>
</table>
```

Dell#

### Example (Summary)

Example (Summary) show ipv6 route summary:

```
Dell# show ipv6 route summary

Route Source        | Active Routes | Non-active Routes |
connected            | 3             | 0                |
static               | 1             | 0                |
Total                | 4             | 0                |
Total 4 active route(s) using 928 bytes
```

Dell#

### 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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>IPv6 Service Class Field</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>111xxxxxx</td>
<td>7</td>
</tr>
<tr>
<td>110xxxxxx</td>
<td>6</td>
</tr>
<tr>
<td>101xxxxxx</td>
<td>5</td>
</tr>
<tr>
<td>100xxxxxx</td>
<td>4</td>
</tr>
<tr>
<td>011xxxxxx</td>
<td>3</td>
</tr>
<tr>
<td>010xxxxxx</td>
<td>2</td>
</tr>
<tr>
<td>001xxxxxx</td>
<td>1</td>
</tr>
<tr>
<td>000xxxxxx</td>
<td>0</td>
</tr>
</tbody>
</table>
Intermediate System to Intermediate System (IS-IS)

IS-IS is an interior gateway protocol that uses shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing through both IP and OSI traffic.

A router is considered as 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 for IPv4 and IPv6. However some command modes might vary when applied to IPv4 and IPv6. These variations have been explicitly explained for such commands. If the variation is not mentioned, then the information applies to both the 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 restart-wait
- graceful-restart t1
- graceful-restart t2
- graceful-restart t3
- hello padding
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)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To perform protocol-support consistency checks on hello packets, use this command. The adjacency-check is enabled by default.

If a BFD session goes down indicating that IPv4 or IPv6 connectivity to its neighbor is lost, it does not imply that the adjacency is lost altogether. The hello adjacency runs over Layer 2, and does not require IP connectivity. However, if IPv4 connectivity is lost to a neighbor, then when the next SPF calculation is performed, the system ensures that it does not calculate any IPv4 or IPv6 routes through that neighbor.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

Syntax

advertise {level1-into-level2 | level2-into-level1} [prefix-list-name]

To return to the default, use the no advertise {level1-into-level2 | level2-into-level1} [prefix-list-name] command.

Parameters

- level1-into-level2: Enter the keywords 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 is enabled.)
- level2-into-level1 (Level 2 to Level 1) leaking is disabled.
Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added IPv6 ISIS support.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Version 6.3.1.0 Introduced</td>
</tr>
</tbody>
</table>

Usage Information

You cannot disable leaking from Level 1 to Level 2. Also, you cannot enable leaking from Level 2 to Level 1. However, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all Level 1 routes are leaked.

You can find more information in IETF RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS.

area-password

Configure a hash message authentication code (HMAC) password for an area.

Syntax

    area-password [hmac-md5 | encryption-type] password

To delete a password, use the no area-password command.

Parameters

- **hmac-md5**
  (OPTIONAL) Enter the keywords hmac-md5 to encrypt the password.
- **encryption-type**
  (OPTIONAL) Enter 7 to encrypt the password using DES.
- **password**
  Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version Description
- **9.8(1.0)** Introduced on the Z9100–ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.5(0.1)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.12.0** Introduced on the S4810.
- **8.3.11.1** Introduced on the Z9000.

**Usage Information**
To prevent the link state database from receiving incorrect routing information from unauthorized routers, use the `area-password` command on routers within an area.

The configured password injects into Level 1 LSPs, CSNPs, and PSNPs.

**Related Commands**
- `domain-password` — set the authentication password for a routing domain.
- `isis password` — configure an authentication password for an interface.

---

### clear config
Clear IS-IS configurations that display under the `router isis` heading of the `show running-config` command output.

**Syntax**
clear config

**Command Modes**
ROUTER ISIS

**Command History**
This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
clear isis

Restart the IS-IS process. All IS-IS data is cleared.

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.

Syntax

```
clear isis [vrf vrf-name] [tag] {* | database | traffic}
```

Parameters

- **vrf vrf-name** (Optional) Enter the keyword vrf followed by the name of the VRF to restart the IS-IS process corresponding to that VRF.
- **tag** (Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
- ***** Enter the keyword * to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.
- **database** Clears IS-IS LSP database information.
- **traffic** Clears IS-IS counters.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

clns host

Define a name-to-network service mapping point (NSAP) that you use with commands that require NSAPs and system IDs.

```
clns host name nsap
```

Parameters

- **name** Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap

Enter a specific NSAP address that is associated with the name parameter.

Defaults
Not configured.

Command Modes
ROUTER ISIS

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

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 — enable dynamic learning of host names from routers in the domain and allows the routers to advertise the host names in LSPs.

diff isis

Enable debugging for all IS-IS operations.

Syntax
diff isis

To disable debugging of IS-IS, use the no diff isis command.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
**debug isis adj-packets**

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

**Syntax**
```
debug isis [vrf vrf-name] adj-packets [interface]
```

To turn off debugging, use the `no debug isis [vrf vrf-name] adj-packets [interface]` command.

**Parameters**
- `vrf vrf-name` (Optional) Enter the keyword `vrf` followed by the name of the VRF to enable the debug information on IS-IS for an adjacency tied to that VRF. This command displays the IIH related debug details.
- `interface` (OPTIONAL) Identifies the interface type and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes**
- EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
debug isis local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

Syntax
debug isis [vrf vrf-name] local-updates [interface]

To turn off debugging, use the no debug isis [vrf vrf-name] updates [interface] command.

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable the debugging information on IS-IS corresponding to that VRF. This information contains local updates tied to the VRF that you specify. This command displays the local LSP debugging details of the current unit.

interface  (OPTIONAL) Identifies the interface type as one of the following:
  • For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  • For a port channel interface, enter the keywords port-channel then a number.
  • For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  Description
9.8(1.0)       Introduced on the Z9100–ON.
9.8(0.0P5)     Introduced on the S4048-ON.
9.8(0.0P2)     Introduced on the S3048-ON.
9.7(0.0)       Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)       Introduced on the Z9500.
9.2(0.2)       Introduced on the Z9000.
9.0.2.0        Introduced on the S6000.
8.3.19.0       Introduced on the S4820T.
8.3.12.0       Introduced on the S4810.
6.3.1.0        Introduced.
**debug isis snp-packets**

To debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets, enable debugging on a specific interface and provides diagnostic information.

**Syntax**

```plaintext
debug isis [vrf vrf-name] snp-packets [interface]
```

To turn off debugging, use the `no debug isis [vrf vrf-name] snp-packets [interface]` command.

**Parameters**

- **vrf vrf-name**
  (Optional) Enter the keyword `vrf` followed by the name of the VRF to enable debugging information on ISIS for CSNP/PSNP packets tied to that VRF. The command displays the SNP (CSNP/PSNP) related debugging information.

- **interface**
  (OPTIONAL) Identifies the interface type as one of the following:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(1.0)
  Introduced on the Z9100-ON.
- 9.8(0.0P5)
  Introduced on the S4048-ON.
- 9.8(0.0P2)
  Introduced on the S3048-ON.
- 9.7(0.0)
  Added support for VRF. Introduced on the S6000-ON.
- 9.5(0.1)
  Introduced on the Z9500.
- 9.2(0.2)
  Introduced on the Z9000.
- 9.0.2.0
  Introduced on the S6000.
- 8.3.19.0
  Introduced on the S4820T.
- 8.3.12.0
  Introduced on the S4810.
- 6.3.1.0
  Introduced.
**debug isis spf-triggers**

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax

```
debug isis [vrf vrf-name] spf-triggers
```

To turn off debugging, use the `no debug isis [vrf vrf-name] spf-triggers` command.

Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable debugging information on IS-IS corresponding to that VRF. This information contains SPF trigger detail tied to the VRF that you specify. When SPF is triggered, this debugging information is displayed.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**debug isis update-packets**

Enable debugging on link state PDUs (LSPs) that a router detects.

Syntax

```
debug isis [vrf vrf-name] update-packets [interface]
```

To turn off debugging, use the `no debug isis update-packets [interface]` command.
Parameters

vrf vrf-name
(UNOPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable the debugging information on IS-IS. This information contains updates from neighbors tied to the VRF that you specify. This command displays the debugging details of the received LSPs from the neighbors.

interface
(UNOPTIONAL) Identifies the interface type and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Added support for VRF. Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.2(0.2) Introduced on the Z9000.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
6.3.1.0 Introduced.

default-information originate
Generates a default route into an IS-IS routing domain and controls the distribution of default information.

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
(UNOPTIONAL) Enter the keyword always to have the default route always advertised.
metric metric
(UNOPTIONAL) Enter the keyword metric then a number to assign to the route. The range is from 0 to 16777215.
route-map map-name
(UNOPTIONAL) A default route the routing process generates if the route map is satisfied.

Defaults
Not configured.
## Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

## Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

- 9.8(1.0) Introduced on the Z9100-ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Introduced on the S6000-ON.
- 9.5(0.1) Introduced on the Z9500.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.12.0 Introduced on the S4810.
- 8.3.11.1 Introduced on the Z9000.
- 7.5.1.0 Added IPv6 ISIS support.
- 6.3.1.0 Introduced.

## Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route advertises depends on the `metric-style` command configuration. If the `metric-style` command is set for Narrow mode and the metric value in the `default-information originate` command is set to a number higher than 63, the metric value advertised in the LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `default-information originate` command is advertised.

## Related Commands

- redistribute — redistribute routes from one routing domain to another routing domain.

---

## description

Enter a description of the IS-IS routing protocol.

**Syntax**

```
description {description}
```

To remove the description, use the `no description {description}` command.

**Parameters**

- `description`: Enter a description to identify the IS-IS protocol (80 characters maximum).

**Defaults**

None

**Command Modes**

- ROUTER ISIS

---

802  | Intermediate System to Intermediate System (IS-IS)
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 the next-hop address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.

- **prefix-list**: (OPTIONAL) Enter the name of a prefix list name.

Defaults

- weight = 115

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>pre-7.7.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Related Commands

- router isis — enter ROUTER mode on the switch.
Usage Information

The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

**distribute-list in**

Filter network prefixes received in updates.

Syntax

distribute-list prefix-list-name in [interface]

To return to the default values, use the no distribute-list prefix-list-name in [interface] command.

Parameters

- **prefix-list-name** Specify the prefix list to filter prefixes in routing updates.
- **interface** (OPTIONAL) Identifies the interface type and the interface following:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
Version | Description
--- | ---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
7.5.1.0 | Added IPv6 ISIS support.
6.3.1.0 | Introduced.

Related Commands
- `distribute-list out` — suppress networks from being advertised in updates.
- `redistribute` — redistribute routes from one routing domain to another routing domain.

### distribute-list out

Suppress network prefixes from being advertised in outbound updates.

**Syntax**

```
distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]
```

To return to the default values, use the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

**Parameters**
- `prefix-list-name` Specify the prefix list to filter prefixes in routing updates.
- `connected` (OPTIONAL) Enter the keyword `connected` for directly connected routing process.
- `ospf process-id` (OPTIONAL) Enter the keyword `ospf` then the OSPF process-ID number. The range is from 1 to 65535.
- `bgp as number` (OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.
- `rip` (OPTIONAL) Enter the keyword `rip` for RIP routes.
- `static` (OPTIONAL) Enter the keyword `static` for user-configured routing process.

**Defaults**
Not configured.

**Command Modes**
- `ROUTER ISIS (for IPv4)`
- `CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)`

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
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` — filter the networks received in updates.
- `redistribute` — redistribute routes from one routing domain to another routing domain.

**distribute-list redistributed-override**

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

**Syntax**
```
distribute-list redistributed-override in
```
To return to the default, use the `no distribute-list redistributed-override in` command.

**Defaults**
none

**Command Modes**
- `ROUTER ISIS (for IPv4)`
- `CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)`

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant `Dell Networking OS Command Line Reference Guide`.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
7.8.1.0 | Added IPv6 ISIS support.
6.3.1.0 | Introduced.
Usage Information

When you execute this command, IS-IS does not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

**domain-password**

Set the authentication password for a routing domain.

**Syntax**

```
domain-password [hmac-md5 | encryption-type] password
```

To disable the password, use the `no domain-password` command.

**Parameters**

- **hmac-md5**
  - (OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.

- **encryption-type**
  - (OPTIONAL) Enter `7` to encrypt the password using DES.

- **password**
  - Enter an alphanumeric string up to 16 characters long. If you do not specify an encryption type or `hmac-md5` keywords, the password is processed as plain text which provides limited security.

**Defaults**

No default password.

**Command Modes**

ROUTER ISIS

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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` — configure an IS-IS area authentication password.
- `isis priority` — configure the authentication password for an interface.

**graceful-restart ietf**

Enable graceful restart on an IS-IS router.

**Syntax**

```
graceful-restart ietf
```

**Usage Information**

Graceful restart prolongs the uptime of a failed system by using a switchover from the failed system to a standby system.
To return to the default, use the `no graceful-restart ietf` command.

### Parameters

- **ietf**
  
Enter `ietf` to enable graceful restart on the IS-IS router.

### Defaults

- Graceful restart disabled.

### Command Modes

- ROUTER ISIS

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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
graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

Syntax

```plaintext
NOTE: Set the t3 timer to adjacency on the restarting router when implementing this command.

graceful-restart restart-wait seconds
```

Parameters

- **seconds**
  
  Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is 30 seconds.

Defaults

- **30 seconds**

Command Modes

- ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Intermediate System to Intermediate System (IS-IS)
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

See Parameters.

Command Modes

- ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.3.1.0 Introduced on the E-Series.

graceful-restart t2

Configure the wait time for the graceful restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

Syntax

```
graceful-restart t2 {level-1 | level-2} seconds
```

Related Commands

- `graceful-restart t3` — configure the overall wait time before graceful restart completes.
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**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---

**graceful-restart t3**

Configure the overall wait time before graceful restart completes.

**Syntax**

```
graceful-restart t3 {adjacency | manual} seconds
```

To return to the default, use the `no graceful-restart t3` command.

**Parameters**

- **adjacency**
  - Enter the keyword `adjacency` so that the restarting router receives the remaining time value from its peer and adjusts its T3 value so if you have configured this option.
- **manual**
  - Enter the keyword `manual` to specify a time value that the restarting router uses. The range is from 50 to 120 seconds. The default is **30 seconds**.

**Defaults**

- **manual, 30 seconds**

**Command Modes**

- **ROUTER ISIS**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*. 
## graceful-restart gracefule-restart

The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command.

Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When you disable `restart-wait`, the current adjacency hold time is used.

Set the t3 timer to `adjacency` on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value so only when you have configured `graceful-restart t3 adjacency`.

### Related Commands

- `graceful-restart restart-wait` — enable the graceful restart maximum wait time before a restarting peer comes up.

### hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

#### Syntax

```
hello padding [multi-point | point-to-point]
```

To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

#### Parameters

- `multi-point` *(OPTIONAL)* Enter the keywords `multi-point` to pad only LAN hello PDUs.
- `point-to-point` *(OPTIONAL)* Enter the keywords `point-to-point` to pad only point-to-point PDUs.

#### Defaults

Both LAN and point-to-point hello PDUs are padded.

#### Command Modes

- `ROUTER ISIS`

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

#### Version

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
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.

**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**

- `isis hello padding` — turn 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**

```plaintext
hostname dynamic
```

To disable this command, use the `no hostname dynamic` command.

**Defaults**

Enabled.

**Command Modes**

ROUTER ISIS

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.

**Usage Information**

To build name-to-systemID mapping tables through the protocol, use this command. All show commands that display systems also display the hostname.

**Related Commands**

- `clns host` — define a name-to-NSAP mapping.
ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax

ignore-lsp-errors

To return to the default values, use the no ignore-lsp-errors command.

Defaults

In IS-IS, the default deletes LSPs with internal checksum errors (no ignore-lsp-errors).

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

IS-IS normally purges LSPs with an incorrect data link checksum causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This process could cause disruption to your system operation.

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

Syntax

ip router isis [tag]

To disable IS-IS on an interface, use the no ip router isis [tag] command.

Parameters

tag (OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

Defaults

No processes are configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

To assign a network entity title to enable IS-IS, use the `net` command.

This command accepts even if an IP address is not configured. This command is cached in the L3 Manager till the IP address is configured. When the IP address configuration reaches the L3Manager, the circuit add message is sent to IS-IS.

**NOTE:** IP address is not mandatory for forming IS-IS adjacency.

**Related Commands**

- `net` — configure an IS-IS network entity title (NET) for the routing process.
- `router isis` — enable the IS-IS routing protocol.

### ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

**Syntax**

```
ipv6 router isis [tag]
```

To disable IS-IS routing, use the `no router isis [tag]` command.

**Parameters**

- `tag` (OPTIONAL) This parameter is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

**Defaults**

Not configured.

**Command Modes**

ROUTER ISIS

**Command History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### Version Description
- **9.0.2.0**: Introduced on the S6000.
- **8.3.19.0**: Introduced on the S4820T.
- **8.3.12.0**: Introduced on the S4810.
- **8.3.11.1**: Introduced on the Z9000.
- **7.5.1.0**: Introduced on the E-Series.

**Usage Information**
Configure a network entity title (the `net` command) to specify the area address and the router system ID.

To establish adjacencies and establish dynamic routing, enable routing on one or more interfaces.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

**Related Commands**
- `net` — configure an IS-IS network entity title (NET) for the routing process.
- `is-type` — assign a type for a given area.

### isis circuit-type

Configure the adjacency type on interfaces.

**Syntax**
```
isis circuit-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, use the `no isis circuit-type` command.

**Parameters**
- **level-1**
  - You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.

- **level-1-2**
  - You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, a Level 2 adjacency is established. This setting is the default.

- **level-2-only**
  - You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

**Defaults**

```
level-1-2
```

**Command Modes**

```
INTERFACE
```

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
**9.8(1.0)** | Introduced on the Z9100–ON.
**9.8(0.0P5)** | Introduced on the S4048-ON.
**9.8(0.0P2)** | Introduced on the S3048-ON.
**9.7(0.0)** | Introduced on the S6000-ON.
**9.5(0.1)** | Introduced on the Z9500.
**isis csnp-interval**

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

**Syntax**

```plaintext
isis csnp-interval seconds [level-1 | level-2]
```

To return to the default values, use the `no isis csnp-interval [seconds] [level-1 | level-2]` command.

**Parameters**

- `seconds`: Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is from 0 to 65535. The default is 10.
- `level-1` (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
- `level-2` (OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

**Defaults**

- `seconds = 10; level-1` (if not otherwise specified)

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.12.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.

**Usage Information**

Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system must be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.
isis hello-interval

Specify the length of time between hello packets sent.

Syntax

```
isis hello-interval seconds [level-1 | level-2]
```

To return to the default values, use the `no isis hello-interval [seconds] [level-1 | level-2]` command.

Parameters

- `seconds` Allows you to set the length of time between hello packet transmissions. The range is from 1 to 65535. The default is 10.
- `level-1` (OPTIONAL) Select this value to configure the hello interval for Level 1. This value is the default.
- `level-2` (OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults

```
seconds = 10; level-1 (if not otherwise specified)
```

Command Modes

- INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

Hello packets are held for a length of three times the value of the hello interval. To conserve bandwidth and CPU usage, use a high hello interval seconds. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands

- `isis hello-multiplier` — specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency as down.
isis hello-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

Syntax

```plaintext
isis hello-multiplier multiplier [level-1 | level-2]
To return to the default values, use the no isis hello-multiplier [multiplier] [level-1 | level-2] command.
```

Parameters

- **multiplier**: Specifies an integer that sets the multiplier for the hello holding time. Never configure a hello-multiplier lower than the default (3). The range is from 3 to 1000. The default is 3.
- **level-1**: (OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
- **level-2**: (OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults

<table>
<thead>
<tr>
<th>multipler</th>
<th>level-1 (if not otherwise specified)</th>
</tr>
</thead>
</table>

Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>INTERFACE</th>
</tr>
</thead>
</table>

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

Related Commands

- `isis hello-interval` — specify the length of time between hello packets.

isis hello padding

Turn ON or OFF padding of hello PDUs from INTERFACE mode.

Syntax

```plaintext
isis hello padding
To return to the default, use the no isis hello padding command.
```
Defaults
Padding of hello PDUs is enabled (ON).

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.

Usage Information
Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF disables padding for the corresponding interface.

Related Commands
• hello padding — turn ON or OFF padding for LAN and point-to-point hello PDUs.

isis ipv6 metric
Assign metric to an interface for use with IPv6 information.

Syntax
isis ipv6 metric default-metric [level-1 | level-2]
To return to the default values, use the no ipv6 isis metric [default-metric] [level-1 | level-2] command.

Parameters
default-metric Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215. The default is 10.

level-1 (OPTIONAL) Enter the keywords level-1 to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This value is the default.

level-2 (OPTIONAL) Enter the keywords level-2 to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults
default-metric = 10; level-1 (if not otherwise specified)

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version Description
- **9.8(1.0)**
  Introduced on the Z9100-ON.
- **9.8(0.0P5)**
  Introduced on the S4048-ON.
- **9.8(0.0P2)**
  Introduced on the S3048-ON.
- **9.7(0.0)**
  Introduced on the S6000-ON.
- **9.5(0.1)**
  Introduced on the Z9500.
- **9.0.2.0**
  Introduced on the S6000.
- **8.3.19.0**
  Introduced on the S4820T.
- **8.3.12.0**
  Introduced on the S4810.
- **8.3.11.1**
  Introduced on the Z9000.
- **7.5.1.0**
  Introduced on the E-Series.

### Usage Information
Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

### isis metric

Assign a metric to an interface.

**Syntax**

```plaintext
isis metric default-metric [level-1 | level-2]
To return to the default values, use the no isis metric [default-metric] [level-1 | level-2] command.
```

**Parameters**

- **default-metric**
  Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215 irrespective of the metric style. The default is **10**.

  If metric value is configured to more than 63, system throughs the following warning:
  ```plaintext
  Warning: for metrics greater than 63, 'metric-style wide' should be configured on level-1-2, or it will be capped at 63.
  ```

  If the metric style is WIDE, the metric values that are greater than 63 are only effective.

- **level-1** (OPTIONAL) Enter the keywords **level-1** to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This setting is the default.

- **level-2** (OPTIONAL) Enter the keywords **level-2** to configure the SPF calculation for Level 2 (inter-area) routing.

**Defaults**

```plaintext
default-metric = 10; level-1 (if not otherwise specified)
```

**Command Modes**

```
INTERFACE
```

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

**Syntax**

```plaintext
isis network point-to-point
```

To disable the feature, use the `no isis network point-to-point` command.

**Defaults**

Not enabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
**isis password**

Configure an authentication password for an interface.

**Syntax**

```plaintext
isis password [hmac-md5] password [level-1 | level-2]
```

To delete a password, use the `no isis password [password] [level-1 | level-2]` command.

**Parameters**

- `encryption-type`
  - (OPTIONAL) Enter `7` to encrypt the password using DES.
- `hmac-md5`
  - (OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
- `password`
  - Assign the interface authentication password.
- `level-1`
  - (OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This setting is the default.
- `level-2`
  - (OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

**Defaults**

No default password. `level-1` (if not otherwise specified).

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the keywords `level-1` and `level-2`.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.
**isis priority**

Set the priority of the designated router you select.

**Syntax**

```plaintext
isis priority value [level-1 | level-2]
```

To return to the default values, use the `no isis priority [value] [level-1 | level-2]` command.

**Parameters**

- `value` This value sets the router priority. The higher the value, the higher the priority. The range is from 0 to 127. The default is 64.
- `level-1` (OPTIONAL) Specify the priority for Level 1. This setting is the default.
- `level-2` (OPTIONAL) Specify the priority for Level 2.

**Defaults**

- `value = 64; level-1` (if not otherwise specified).

**Command Modes**

`INTERFACE`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN is the designated router. Priorities are advertised within hellos. The router with the highest priority becomes the designated intermediate system (DIS).

**NOTE:** Routers with a priority of 0 cannot be a designated router.

Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address becomes DIS even though its priority is 0.

---

**is-type**

Configure IS-IS operating level for a router.

**Syntax**

```plaintext
is-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, use the `no is-type` command.
**Parameters**

- **level-1**  Allows a router to act as a Level 1 router.
- **level-1-2**  Allows a router to act as both a Level 1 and Level 2 router. This setting is the default.
- **level-2-only**  Allows a router to act as a Level 2 router.

**Defaults**  
**level-1-2**

**Command Modes**  
ROUTER ISIS

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**  
The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. You can configure the IS type as Level 1.

---

**log-adjacency-changes**

Generate a log messages for adjacency state changes.

**Syntax**  
log-adjacency-changes

To disable this function, use the no log-adjacency-changes command.

**Defaults**  
Adjacency changes are not logged.

**Command Modes**  
ROUTER ISIS

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
**lsp-gen-interval**

Set the minimum interval between successive generations of link-state packets (LSPs).

**Syntax**

```
lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the `no lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

**Parameters**

- **level-1** (OPTIONAL) Enter the keywords level-1 to apply the configuration to generation of Level-1 LSPs.
- **level-2** (OPTIONAL) Enter the keywords level-2 to apply the configuration to generation of Level-2 LSPs.
- **interval seconds** Enter the maximum number of seconds between LSP generations. The range is from 0 to 120 seconds. The default is **5 seconds**.
- **initial_wait_interval seconds** (OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. The range is from 0 to 120 seconds. The default is **1 second**.
- **second_wait_interval seconds** (OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. The range is from 0 to 120 seconds. The default is **5 seconds**.

**Defaults**

See Parameters.

**Command Modes**

ROUTER ISIS

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.

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.
Usage Information

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (interval seconds). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs this router generates.

Syntax

```
lsp-mtu size
```

To return to the default values, use the `no` `lsp-mtu` command.

Parameters

- `size`: The maximum LSP size, in bytes. The range is from 512 to 16000 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is 1497.

**NOTE**: The appropriate interface circuit is brought down and removed.

Defaults

1497 bytes.

Command Modes

- ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
7.5.1.0 | Added support for LSP Throttling Enhancement.

Usage Information
The link MTU and the LSP MTU size must be the same.

Because each device can generate a maximum of 255 LSPs, consider carefully whether you use the `lsp-mtu` command.

**lsp-refresh-interval**

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their `max-lsp-lifetime` reaches zero and then LSPs is purged.

**Syntax**
```
  lsp-refresh-interval  seconds
```
To restore the default refresh interval, use the `no lsp-refresh-interval` command.

**Parameters**
- **seconds**
  - The LSP refresh interval, in seconds. This value must be 300 seconds less than the value specified in the `max-lsp-lifetime` command. The range is from 1 to 65535 seconds. The default is 900.

**Defaults**
900 seconds

**Command Modes**
ROUTER ISIS

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for LSP Throttling Enhancement.</td>
</tr>
</tbody>
</table>

**Usage Information**
The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the `max-lsp-lifetime` command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization the flooding of refreshed packets causes.
max-area-addresses

Configure manual area addresses.

Syntax

max-area-addresses number

To return to the default values, use the no max-area-addresses command.

Parameters

- **number**: Set the maximum number of manual area addresses. The range is from 3 to 6. The default is 3.

Defaults

3 addresses

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for LSP Throttling Enhancement.</td>
</tr>
</tbody>
</table>

Usage Information

To configure the number of area addresses on router, use this command. This value must be consistent with routers in the same area, otherwise the router forms only Level 2 adjacencies. The value must be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax

max-lsp-lifetime seconds

To restore the default time, use the no max-lsp-lifetime command.
The maximum lifetime of LSP in seconds. This value must be greater than the `lsp-refresh-interval` command. The higher the value the longer the LSPs are kept. The range is from 1 to 65535. The default is `1200`.

**Defaults**
- 1200 seconds

**Command Modes**
- ROUTER ISIS

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**
Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The `seconds` parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

**Related Commands**
- `lsp-refresh-interval` — set the link-state packet (LSP) refresh interval.

### maximum-paths

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

**NOTE:** Enables you to configure a single system wide value that is common for both IPv4 and IPv6 addresses.

**Syntax**
```
maximum-paths number
```

To return to the default values, use the `no maximum-paths` command.

**Parameters**
- `number` Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is from 1 to 64. The default is 4.

**Defaults**
- 4

**Command Modes**
- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)
**metric-style**

To generate and accept old-style, new-style, or both styles of type, length, and values (TLV), configure a router.

**Syntax**

```
metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]
```

To return to the default values, use the `no metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]` command.

**Parameters**

- `narrow` Allows you to generate and accept old-style TLVs. The metric range is from 0 to 63.
- `transition` Allows you to generate both old-style and new-style TLVs. The metric range is from 0 to 63.
- `wide` Allows you to generate and accept only new-style TLVs. The metric range is from 0 to 16777215.
- `level-1` Enables the metric style on Level 1.
- `level-2` Enables the metric style on Level 2.

**Defaults**

- `narrow`: if no Level is specified, Level-1 and Level-2 are configured.

**Command Modes**

- `ROUTER ISIS`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for multi-topology ISIS.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>
### Usage Information

If you enter the `metric-style wide` command, the Dell Networking OS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

When wide transition is configured, narrow metric is sent for the narrow metric TLV and the actual wide metric is sent in wide metric TLV. The receiver can choose to use the metric that is requires.

**Related Commands**

- `isis metric` — configure a metric for an interface.

### multi-topology

Enables multi-topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

**Syntax**

```
multi-topology [transition]
```

To return to a single topology configuration, use the `no multi-topology [transition]` command.

**Parameters**

- `transition`:

**Defaults**

Disabled

**Command Modes**

CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### net

To configure an IS-IS network entity title (NET) for a routing process, use this mandatory command. If you did not configure a NET, the IS-IS process does not start.

**Syntax**

```
net network-entity-title
```

To remove a net, use the `no net network-entity-title` command.

**Parameters**

- `network-entity-title` Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

**Defaults**

Not configured.

**Command Modes**

- ROUTER ISIS

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

### 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 the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

`ROUTER ISIS`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

Although the passive interface does not send nor receive routing updates, the network on that interface is still included in the IS-IS updates sent using other interfaces.

---

**redistribute**

Redistribute routes from one routing domain to another routing domain.

**Syntax**

```
redistribute {static | connected | rip} [level-1 | level-1-2 | level-2] [metric metric-value] [metric-type {external | internal}] [route-map map-name]
```

To end redistribution or disable any of the specified keywords, use the `no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name]` command.

**Parameters**

- `connected`
  - Enter the keyword `connected` to redistribute active routes into IS-IS.
- `rip`
  - Enter the keyword `rip` to redistribute RIP routes into IS-IS.
- `static`
  - Enter the keyword `static` to redistribute user-configured routes into IS-IS.
- `metric metric-value`
  - (OPTIONAL) Assign a value to the redistributed route. The range is from 0 to 16777215. The default is 0. Use a value that is consistent with the destination protocol.
- `metric-type {external | internal}`
  - (OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following:
    - `external`
    - `internal`
internal

level-1 (OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2 (OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.

level-2 (OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.

route-map map-name (OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routes are imported.

Defaults

- metric metric-value = 0
- metric-type= internal; level-2

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for IPv6 ISIS.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

To redistribute a default route (0.0.0.0/0), configure the default-information originate command.

Changing or disabling a keyword in this command does not affect the state of the other command keywords.

When an LSP with an internal metric is received, the Dell Networking OS considers the route cost while considering the advertised cost to reach the destination.

Redistributed routing information is filtered with the distribute-list out command to ensure that the routes are properly passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the metric-style command. If the metric-style command is set for Narrow or Transition mode and the metric value in the redistribute command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the metric-style command is set for Wide mode, the metric value in the redistribute command is advertised.
Related Commands

- `default-information originate` — generate a default route for the IS-IS domain.
- `distribute-list out` — suppress networks from being advertised in updates. This command filters redistributed routing information.

**redistribute bgp**

Redistribute routing information from a BGP process.

**Syntax**

```
redistribute bgp AS number [level-1 | level-1-2 | level-2] [metric metric-value] [metric-type {external| internal}] [route-map map-name]
```

To return to the default values, use the `no redistribute bgp` command with the appropriate parameters.

**Parameters**

- **AS number**: Enter a number that corresponds to the autonomous system number. The range is from 1 to 65535.
- **level-1** (OPTIONAL): Routes are independently redistributed into IS-IS Level 1 routes only.
- **level-1-2** (OPTIONAL): Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
- **level-2** (OPTIONAL): Routes are independently redistributed into IS-IS as Level 2 routes only. This setting is the default.
- **metric metric-value** (OPTIONAL): The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is 0.
- **metric-type** (OPTIONAL): The external link type associated with the default route advertised into a routing domain. The two options are:
  - `external`
  - `internal`
- **route-map map-name**: map-name is an identifier for a configured route map. The route map filters imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

**Defaults**

IS-IS Level 2 routes only

**Command Modes**

- `ROUTER ISIS (for IPv4)`
- `CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
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

process-id
Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.

metric metric-value
(Optional) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is 0.

metric-type {external | internal}
(Optional) The external link type associated with the default route advertised into a routing domain. The two options are:

- external
- internal

level-1
(Optional) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2
(Optional) Routes are independently redistributed into IS-IS as Level-1-2 routes.

level-2
(Optional) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
match (external | internal) (OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are
- internal
- external

route-map map-name map-name is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol.
If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults
See Parameters.

Command Modes
- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for IPv6 ISIS.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information
How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the metric-style command. If the metric-style command is set for Narrow mode and the metric value in the redistribute ospf command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the metric-style command is set for wide mode, the metric value in the redistribute ospf command is advertised.

router isis

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Syntax
router isis [vrf vrf-name] [tag]
To disable IS-IS routing, use the `no router isis [tag]` command.

**Parameters**
- **vrf vrf-name**
  - Enter the keyword `vrf` followed by the name of the VRF to enable the IS-IS routing protocol and to specify an IP IS-IS process on that VRF.
- **tag**
  - (OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the `tag` option is not specified. The tag name must be unique for all IP router processes for a given router.

**Defaults**
- Not configured.

**Command Modes**
- CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**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` — configure IS-IS routing processes for IP on interfaces and attaches an area designator to the routing process.
- `net` — configure an IS-IS network entity title (NET) for a routing process.
- `is-type` — assign a type for a given area.

### set-overload-bit

To set the overload bit in zeroth fragment of non-pseudonode LSPs on the router, configure the router. This setting prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

**Syntax**
```
set-overload-bit
```

To return to the default values, use the `no set-overload-bit` command.

**Defaults**
- Not set.
Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for multi-topology ISIS.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

**NOTE:** Enables you to configure a single system wide value that is common for both IPv4 and IPv6 address.

**show config**

Display the changes you made to the IS-IS configuration. Default values are not shown.

**Syntax**

```
show config
```

**Command Modes**

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>


Version | Description
---|---
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.1 | Introduced on the S4810.

Example (Router-Isis) The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

Dell(conf-router_isis)# show config
! router isis
cns host ISIS 49.0000.0001.F100.E120.0013.00
log-adjacency-changes
net 49.0000.0001.F100.E120.0013.00
! address-family ipv6 unicast
maximum-paths 16
**multi-topology transition**
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family

Example (Address-Family_IPv6) The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

Dell(conf-router_isis-af_ipv6)# show conf
! address-family ipv6 unicast
maximum-paths 16
**multi-topology transition**
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family

**show isis database**

Display the IS-IS link state database.

**Syntax**

```
show isis [vrf vrf-name] database [level-1 | level-2] [local] [detail | summary] [system-id] [lspid]
```

**Parameters**

- **vrf vrf-name** (Optional) Enter the keyword vrf followed by the name of the VRF to display IS-IS link state database corresponding to that VRF.

  **NOTE:** If you do not specify this option, the IS-IS link state database corresponding to the default VRF are displayed.

- **level-1** (OPTIONAL) Displays the Level 1 IS-IS link-state database.

- **level-2** (OPTIONAL) Displays the Level 2 IS-IS link-state database.

- **local** (OPTIONAL) Displays local link-state database information.
detail (OPTIONAL) Displays the detailed link-state database information of each LSP when specified. If not specified, a summary displays.

summary (OPTIONAL) Displays the summary of link-state database information when specified.

lspid (OPTIONAL) Display only the specified LSP.

system-id (OPTIONAL) Displays the link-state database for system-id.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Added supported for VRF. Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.2(0.2) Introduced on the Z9000.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.7.1 Introduced on the S4810.

Usage Information

The following describes the show isis database command shown in the following example.

Field Description
IS-IS Level-1/Level-2 Link State Database Displays the IS-IS link state database for Level 1 or Level 2.
LSPID Displays the LSP identifier.
The first six octets are the System ID of the originating router.
The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, the LSP describes system links. If this byte is zero (0), the LSP describes the state of the originating router.
The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems.
The last octet is the LSP number. An LSP is divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number.
An * after the LSPID indicates that the system originates an LSP where this command was issued.
LSP Seq Num This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
**Field**  | **Description**  
--- | ---  
LSP Checksum | This is the checksum of the entire LSP packet.  
LSP Holdtime | This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.  
ATT | This value represents the Attach bit. This value indicates that the router is a Level 1-2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 1-2 routers use the Attach bit to find the closest Level 1-2 router. They install a default route to the closest Level 1-2 router.  
P | This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.  
OL | This value represents the overload bit, determining congestion. If the overload bit is set, other routers do not use this system as a transit router when calculating routes.  

**Example**  
The bold sections identify that MultiTopology IS-IS is enabled.

```
Dell# show isis database
IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0

Dell# show isis database detail ISIS.00-00
IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002B 0x853B    1075         0/0/0
Area Address: 49.0000.0001  
NLPID: 0xCC 0x8E  
IP Address: 10.1.1.1  
IPv6 Address: 1011::1  
Topology: IPv4 (0x00) IPv6 (0x8002)  
Metric: 10    IS OSPF.00  
Metric: 10    IS (MT-IPv6) OSPF.00  
Metric: 10    IP 15.1.1.0 255.255.255.0  
Metric: 10    IPv6 (MT-IPv6) 1511::/64  
Metric: 10    IPv6 (MT-IPv6) 2511::/64  
Metric: 10    IPv6 (MT-IPv6) 1011::/64  
Metric: 10    IP 10.1.1.0 255.255.255.0  
Metric: 10    IPv6 1511::/64  
Metric: 10    IPv6 (MT-IPv6) 1011::/64  
Metric: 10    IPv6 2511::/64  
Metric: 10    IPv6 (MT-IPv6) 1011::/64  
Metric: 10    IPv6 (MT-IPv6) 2511::/64
Hostname: ISIS

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000002D 0x82CD    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: 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
```
**show isis graceful-restart detail**

Display detailed IS-IS graceful restart related settings.

**Syntax**

```
show isis [vrf vrf-name] graceful-restart detail
```

**Command Modes**

- EXEC
- EXEC Privilege

**Parameters**

- `vrf vrf-name` (Optional) Enter the keyword vrf followed by the name if the VRF to display IS-IS graceful restart details corresponding to that VRF.

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show isis graceful-restart detail
Configured Timer Value
======================
Graceful Restart    : Enabled
T3 Timer            : Manual
```
T3 Timeout Value : 30
T2 Timeout Value : 30 (level-1), 30 (level-2)
T1 Timeout Value : 5, retry count: 1
Adjacency wait time : 30

Operational Timer Value
======================
Current Mode/State : Normal/RUNNING
T3 Time left : 0
T2 Time left : 0 (level-1), 0 (level-2)
Restart ACK rcv count : 0 (level-1), 0 (level-2)
Restart Req rcv count : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
Database Sync count : 0 (level-1), 0 (level-2)

show isis hostname

Display IS-IS host names configured or learned on the switch.

Syntax

show isis [vrf vrf-name] hostname

Parameters

vrf vrf-name Enter the keyword vrf followed by the name of the VRF to display IS-IS host names corresponding to that VRF.

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Added support for VRF. Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.

Example

Dell# show isis hostname
System Id Dynamic Name Static Name
*F100.E120.0013 Force10 ISIS
Dell#
show isis interface

Display detailed IS-IS interface status and configuration information.

Syntax

```
show isis [vrf vrf-name] interface [interface]
```  

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display IS-IS interface status information corresponding to that VRF.
- `interface` (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on</td>
</tr>
<tr>
<td></td>
<td>the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Example

```
Dell> show isis int
GigabitEthernet 1/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
    Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
```
Number of active level-1 adjacencies: 1
Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-1 Hello in 2 seconds
Next IS-IS LAN Level-2 Hello in 1 seconds
LSP Interval: 33
GigabitEthernet 1/0 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

show isis neighbors

Display information about neighboring (adjacent) routers.

**Syntax**

```
show isis [vrf vrf-name] neighbors [level-1 | level-2] [detail] [interface]
```

**Parameters**

- **vrf vrf-name**  
  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display adjacent router information corresponding to that VRF.

- **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 the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
### Version Description
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Added support for VRF. Introduced on the S6000-ON.
- 9.5(0.1) Introduced on the Z9500.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.12.0 Introduced on the S4810.
- 8.3.11.1 Introduced on the Z9000.

### Usage Information
Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

The following describes the `show isis neighbors` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The value that identifies a system in an area.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface, slot, and port in which the router was discovered.</td>
</tr>
<tr>
<td>State</td>
<td>The value providing status about the adjacency state. The range is Up and Init.</td>
</tr>
<tr>
<td>Type</td>
<td>This value displays the adjacency type (Layer 2, Layer 2 or both).</td>
</tr>
<tr>
<td>Priority</td>
<td>IS-IS priority the neighbor advertises. The neighbor with highest priority becomes the designated router for the interface.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Displays the interfaces uptime.</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The neighbor’s interpretation of the designated router for the interface.</td>
</tr>
</tbody>
</table>

### Example
The bold sections below identify that Multi-Topology IS-IS is enabled. This command displays only one IP address per line.

```
Dell# show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2 (M) 127 09:28:01 TEST.02
!
Dell# show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2 (M) 127 09:28:04 TEST.02 Area Address(es): 49.0000.0001
   IP Address(es): 25.1.1.3*
   MAC Address: 0000.0000.0000
   Hold Time: 28
   Link Local Address: fe80::201:e8ff:fe00:492c
   Topology: IPv4 IPv6, Common (IPv4 IPv6)
   Adjacency being used for MTs: IPv4 IPv6
Dell#
```
**show isis protocol**

Display IS-IS routing information.

**Syntax**

gshow isis [vrf vrf-name] protocol

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display IS-IS routing information corresponding to that VRF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Example**

The bold section identifies that Multi-Topology IS-IS is enabled.

```
Dell# show isis protocol
IS-IS Router: <Null Tag>
    System Id: F100.E120.0013 IS-Type: level-1-2
    Manual area address(es):
        49.0000.0001
    Routing for area address(es):
        49.0000.0001
    Interfaces supported by IS-IS:
        GigabitEthernet 1/1 - IP - IPv6
        GigabitEthernet 1/2 - IP - IPv6
        GigabitEthernet 1/10 - IP - IPv6
    Loopback 0 - IP - IPv6
    Redistributing:
    Distance: 115
    Generate narrow metrics: level-1-2
    Accept narrow metrics: level-1-2
    Generate wide metrics: none
    Accept wide metrics: none
```
show isis traffic

This command allows you to display IS-IS traffic interface information.

Syntax

show isis [vrf vrf-name] traffic [interface]

Parameters

vrf vrf-name (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display IS-IS traffic interface information corresponding to that VRF.

interface (OPTIONAL) Identifies the interface type and the interface following:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Added support for VRF. Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.2(0.2) Introduced on the Z9000.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.

Usage Information

The following describes the show isis traffic command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level-1/Level-2</td>
<td>Displays the number of Hello packets sent and received.</td>
</tr>
<tr>
<td>Hellos (sent/rcvd)</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PTP Hellos (sent/rcvd)</td>
<td>Displays the number of point-to-point Hellos sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs sourced (new/refresh)</td>
<td>Displays the number of new and refreshed LSPs.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs flooded (sent/rcvd)</td>
<td>Displays the number of flooded LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs CSNPs (sent/rcvd)</td>
<td>Displays the number of CSNP LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 LSPs PSNPs (sent/rcvd)</td>
<td>Displays the number of PSNP LSPs sent and received.</td>
</tr>
<tr>
<td>Level-1/Level-2 DR Elections</td>
<td>Displays the number of times designated router elections ran.</td>
</tr>
<tr>
<td>Level-1/Level-2 SPF Calculations</td>
<td>Displays the number of shortest path first calculations.</td>
</tr>
<tr>
<td>LSP checksum errors received</td>
<td>Displays the number of checksum errors LSPs received.</td>
</tr>
<tr>
<td>LSP authentication failures</td>
<td>Displays the number of LSP authentication failures.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show is traffic
IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
IS-IS: PTP Hellos (sent/rcvd) : 0/0
IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
IS-IS: Level-1 DR Elections : 4
IS-IS: Level-2 DR Elections : 4
IS-IS: Level-1 SPF Calculations : 0
IS-IS: Level-2 SPF Calculations : 389
IS-IS: LSP checksum errors received : 0
IS-IS: LSP authentication failures : 0
Dell#
```

**spf-interval**

Specify the minimum interval between shortest path first (SPF) calculations.

**Syntax**

```
spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]
```

To restore default values, use the no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]] command.
Parameters

- **level-l** (OPTIONAL) Enter the keyword level-l to apply the configuration to Level-1 SPF calculations.
- **level-2** (OPTIONAL) Enter the keyword level-2 to apply the configuration to Level-2 SPF calculations.
- **interval seconds** Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is **10 seconds**.
- **initial_wait_interval seconds** (OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.
- **second_wait_interval seconds** (OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.

Defaults

See Parameters.

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for multi-topology ISIS.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for SPF Throttling Enhancement.</td>
</tr>
</tbody>
</table>

Usage Information

This command spf-interval in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using Single Topology mode, use the spf-interval command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculations are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (interval seconds). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).
Link Aggregation Control Protocol (LACP)

This section contains commands for Dell Networks’ implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs) — known as “port-channels” in the Dell Networking OS.

**NOTE:** For static LAG commands based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, see Port Channel Commands.

Topics:
- clear lacp counters
- debug lacp
- lacp long-timeout
- lacp port-priority
- lacp system-priority
- port-channel-protocol lacp
- show lacp

### clear lacp counters

Clear port channel counters.

**Syntax**

```plaintext
clear lacp port-channel-number counters
```

**Parameters**

- `port-channel-number` Enter a port-channel number. The range is from 1 to 128.

**Defaults**

Without a Port Channel specified, the command clears all Port Channel counters.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
</tbody>
</table>
### debug lacp

Debug LACP (configuration, events, and so on).

**Syntax**

```
debug lacp [config | events | pdu [interface-type [in | out]]]
```

To disable LACP debugging, use the `no [config | events | pdu [interface-type [in | out]]]` command.

**Parameters**

- `config` (OPTIONAL) Enter the keyword `config` to debug the LACP configuration.
- `events` (OPTIONAL) Enter the keyword `events` to debug the LACP event information.
- `pdu` (OPTIONAL) Enter the keyword `pdu` to debug the LACP Protocol Data Unit information.
- `interface-type in | out` (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Optionally, enter an `in` or `out` parameter:

- Receive enter `in`
- Transmit enter `out`

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

**Syntax**

```
lacp long-timeout
```

To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.

**Defaults**

1 second

**Command Modes**

INTERFACE (conf-if-po-number)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
### 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**

```plaintext
lacp port-priority priority-value
```

To return to the default setting, use the `no lacp port-priority priority-value` command.

**Parameters**

- **priority-value**: Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

**Defaults**

- **32768**

**Command Modes**

- **INTERFACE**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

**Version**

- **9.8(1.0)**: Introduced on the Z9100–ON.
- **9.8(0.0P5)**: Introduced on the S4048-ON.
- **9.8(0.0P2)**: Introduced on the S3048-ON.
- **9.7(0.0)**: Introduced on the S6000–ON.
- **9.2(1.0)**: Introduced on the Z9500.
- **9.0.2.0**: Introduced on the S6000.
- **8.3.19.0**: Introduced on the S4820T.
- **8.3.11.1**: Introduced on the Z9000.
- **8.3.7.0**: Introduced on the S4810.
- **7.6.1.0**: Introduced on the S-Series.
- **7.5.1.0**: Introduced on the C-Series.
lacp system-priority

Configure the LACP system priority.

Syntax

```
lacp system-priority priority-value
```

Parameters

- `priority-value` Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults

**32768**

Command Modes

**INTERFACE**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

port-channel-protocol lacp

Enable LACP on any LAN port.

Syntax

```
port-channel-protocol lacp
```

Link Aggregation Control Protocol (LACP)
To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

### Command Modes
```
INTERFACE
```

### Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Related Commands
- `show lacp` — display the LACP information.
- `show interfaces port-channel` — display information on configured Port Channel groups.

## show lacp

Display the LACP matrix.

### Syntax
```
show lacp port-channel-number [sys-id | counters]
```

### Parameters

- **port-channel-number**: Enter a port-channel number. The range is from 1 to 128.
- **sys-id**: (OPTIONAL) Enter the keywords `sys-id` and the value that identifies a system.
- **counters**: (OPTIONAL) Enter the keyword `counters` to display the LACP counters.

### Defaults
Without a Port Channel specified, the command clears all Port Channel counters.

### Command Modes
```
• EXEC
• EXEC Privilege
```

### Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.2.1.1 | Introduced on the E-Series.

Example (Port-Channel-Number)

```
Dell# show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID:Priority 32768, Address 0001.e800.a12b
Partner System ID:Priority 32768, Address 0001.e801.45a5
   Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
   LACP LAG 1 is an aggregatable link

A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-OUT_OF_SYNC
I-Collection enabled, J-Collection disabled, K-Distribution enabled
L-Distribution disabled, M-Partner Defaulted, N-Partner Non-defaulted, O-Receiver is in expired state,
P-Receiver is not in expired state

Port Gi 1/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1 Priority 128
        Oper: State ACEGIKNP Key 1 Priority 128
  Partner Admin: State BDFHJLMP Key 0 Priority 0
        Oper: State BCEGIKNP Key 1 Priority 128

Dell#
```

Example (Sys-id)

```
Dell# show lacp 1 sys-id
Actor   System ID: Priority 32768, Address 0001.e800.a12b
Partner  System ID: Priority 32768, Address 0001.e801.45a5

Dell#
```

Example (Counter)

```
Dell# show lacp 1 counters
----------------------------------------------------
Port     LACP PDU  Marker PDU  Unknown   Illegal
         Xmit Recv  Xmit Recv  Pkts Rx   Pkts Rx
----------------------------------------------------
Gi 1/6    200  200     0    0        0          0

Dell#
```

Related Commands

- clear lacp counters — clear the LACP counters.
- show interfaces port-channel — display information on configured Port Channel groups.
This section describes commands to configure Layer 2 features.

### MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

#### clear mac-address-table

Clear the MAC address table of all MAC address learned dynamically.

**Syntax**

```
clear mac-address-table {dynamic | sticky }{address mac-address | all | interface interface | vlan vlan-id}
```

**Parameters**

- `dynamic` Enter the keyword `dynamic` to specify dynamically-learned MAC addresses.
- `sticky` Enter the keyword `sticky` to specify sticky MAC addresses.
- `address mac-address` Enter the keyword `address` then a MAC address in nn:nn:nn:nn:nn:nn format.
- `all` Enter the keyword `all` to delete all MAC address entries in the MAC address table.
- `interface interface` Enter the following keywords and slot/port or number information:
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - 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.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Added support for sticky MAC addresses.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

Syntax

```
mac-address-table aging-time seconds
```

Parameters

- `seconds` Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter 0. The range is from 10 to 1000000. The default is 1800 seconds.

Defaults

1800 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>On the E-Series, available in INTERFACE VLAN context, reduced the minimum aging time in the INTERFACE VLAN context from 10 seconds to 1 second.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `mac learning-limit` — set the MAC address learning limits for a selected interface.
show mac-address-table aging-time — display the MAC aging time.

mac-address-table disable-learning

Disable MAC address learning from LACP or LLDP BPDUs.

Syntax

mac-address-table disable-learning [lacp | lldp]

Parameters

- lacp: Enter lacp to disable MAC address learning from LACP BPDUs.
- lldp: Enter LLDP to disable MAC address learning from LLDP BPDUs.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S3048-ON, S3100 series, S4048-ON, S4810, S4820T, S5000, S6000, S6000-ON, Z9100-ON, and Z9500.

Usage Information

If you use the `mac-address-table disable-learning` command without specifying any option, the system does not learn source MAC addresses from LACP or LLDP BPDUs.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and VLANs.

Syntax

mac-address-table static mac-address {multicast vlan vlan-id output-range interface}{output interface vlan vlan-id}

To remove a MAC address, use the `no mac-address-table static mac-address output interface vlan vlan-id` command.

Parameters

- `multicast`: Enter a vlan port to which L2 multicast MAC traffic is forwarded.

**NOTE:** Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.

- `output interface`: For a unicast MAC address, enter the keyword `output` then one of the following interfaces for which traffic is forwarded:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

- For a port channel interface, enter the keywords port-channel then a number.

**output-range**

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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.

**vlan vlan-id**
Enter the keyword vlan then a VLAN ID number from 1 to 4094.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(0.0P5) |Introduced on the S4048-ON.
9.8(0.0P2) |Introduced on the S3048-ON.
9.7(0.0) |Introduced on the S6000–ON.
9.2(1.0) |Introduced on the Z9500.
9.0.2.0 |Introduced on the S6000.
9.1(0.0) |Added support for output range parameter for S4810 and Z9000.
8.3.19.0 |Introduced on the S4820T.
8.3.11.1 |Introduced on the Z9000.
8.5.1.0 |Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 |Introduced on the S4810.
7.6.1.0 |Introduced on the S-Series.
7.5.1.0 |Introduced on the C-Series.
pre-6.2.1.1 |Introduced on the E-Series.

**Example (Unicast)**

mac-address-table static 00:01:00:00:00:01 {output Gi 1/2 vlan 2}

**Example (Multicast)**

mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output-range Gi 1/2, Gi 1/3}

**Related Commands**

- **show mac-address-table** — display the MAC address table.
mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

Syntax

mac-address-table station-move refresh-arp

To disable the ARP refresh feature, use the no mac-address-table station-move refresh-arp command.

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Modified the default option from none to Enabled.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

For more information about using this command, see NIC Teaming in the Layer 2 section of the Dell Networking OS Configuration Guide.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

Syntax

mac learning-limit address_limit [vlan vlan-id] [station-move-violation [dynamic]] [dynamic [no-station-move| station-move]]

Parameters

- `address_limit`: Enter the maximum number of MAC addresses that can be learned on the interface. The range is from 1 to 1000000.
vlan vlan-id
  Enter the keyword then the VLAN ID. The range is from 1 to 4094.

dynamic
  (OPTIONAL) Enter the keyword dynamic to allow aging of MACs even though a
  learning limit is configured.

station-move-violation
  (OPTIONAL) Enter the keywords station-move to allow a station move on learned
  MAC addresses.

 Defaults
  • On S-Series, the default behavior is dynamic.

  NOTE: “Static” means manually entered addresses, which do not age.

 Command Modes
  INTERFACE

 Command History
  This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
  OS Command Line Reference Guide.

  Version     Description
  9.8(1.0)    Introduced on the Z9100–ON.
  9.8(0.0P5)  Introduced on the S4048-ON.
  9.8(0.0P2)  Introduced on the S3048-ON.
  9.7(0.0)    Introduced on the S6000-ON.
  9.2(1.0)    Introduced on the Z9500.
  9.0.2.0     Introduced on the S6000.
  8.3.19.0    Introduced on the S4820T.
  8.3.11.1    Introduced on the Z9000.
  8.3.12.0    Deprecated the no-station-move command (replaced by the mac-learning-
               limit mac-address-sticky command).
  8.3.7.0     Introduced on the S4810.
  8.3.1.0     Added the vlan option on the E-Series.
  8.2.1.0     Introduced on the S-Series.
  7.7.1.0     Introduced on the C-Series. Added the station-move option.
  6.5.1.0     Added support for MAC Learning-Limit on the LAG.

 Usage Information
  This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

  If you do not specify the vlan option, the MAC address counters are not VLAN-based. That is, the sum of the
  addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning
  limit.

  MAC Learning Limit violation logs and actions are not available on a per-VLAN basis.

  With the keyword no-station-move option, MAC addresses learned through this feature on the selected
  interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no
  effect on already learned MAC addresses.

  After the MAC address learning limit is reached, the MAC addresses do not age out unless you add the dynamic
  option. To clear statistics on MAC address learning, use the clear counters command with the learning-limit
  parameter.
NOTE: If you configure this command on an interface in a routed VLAN, and after the MAC addresses learned reaches the limit set in the `mac learning-limit` command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

- `mac learning-limit mac-address-sticky` — replace deprecated no-station-move parameter.
- `show mac learning-limit` — display MAC learning-limit configuration.

**mac learning-limit learn-limit-violation**

Configure an action for a MAC address learning-limit violation.

```
mac learning-limit learn-limit-violation {log | shutdown}
```

To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.

**Syntax**

- `log` — Enter the keyword `log` to generate a syslog message on a learning-limit violation.
- `shutdown` — Enter the keyword `shutdown` to shut down the port on a learning-limit violation.

**Defaults**

None

**Command Modes**

INTERFACE (conf-if-interface-slot/port)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Usage Information

This command is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands

- **show mac learning-limit** — display details of the mac learning-limit.

---

### mac learning-limit mac-address-sticky

Maintain the dynamically learned mac addresses as sticky MAC addresses on the selected port.

#### Syntax

```
mac learning-limit mac-address-sticky
```

To convert the sticky MAC addresses to dynamic MAC addresses, use the `no mac learning-limit` command.

#### Parameters

- **mac-address-sticky**  Configures the dynamic MAC addresses as sticky on an interface.

#### Defaults

None

#### Command Modes

INTERFACE

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

#### Usage Information

If you configure `mac-learn-limit` and the sticky MAC feature is enabled, dynamically learned MAC addresses are converted to sticky for that port. Any new MAC address that is learned also becomes sticky for that port.

#### Related Commands

- **show mac learning-limit** — display the details of the mac learning-limit.
**mac learning-limit station-move-violation**

Specify the actions for a station move violation.

**Syntax**

```
mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}
```

To disable a configuration, use the `no mac learning-limit station-move-violation` command, then the configured keyword.

**Parameters**

- **log**
  - Enter the keyword `log` to generate a syslog message on a station move violation.

- **shutdown-both**
  - Enter the keyword `shutdown` to shut down both the original and offending interface and generate a syslog message.

- **shutdown-offending**
  - Enter the keywords `shutdown-offending` to shut down the offending interface and generate a syslog message.

- **shutdown-original**
  - Enter the keywords `shutdown-original` to shut down the original interface and generate a syslog message.

**Defaults**

None

**Command Modes**

INTERFACE (conf-if-interface-slot/port)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command is supported on physical interfaces, static LAGs, and LACP LAGs.

**Related Commands**

- `show mac learning-limit` — display details of the mac learning-limit.
**mac learning-limit reset**

Reset the MAC address learning-limit error-disabled state.

**Syntax**

```
mac learning-limit reset
```

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**show cam mac linecard (count)**

Display the content addressable memory (CAM) size and the portions allocated for MAC addresses and for MAC ACLs.

**Syntax**

```
show cam mac linecard slot port-set port-pipe count [vlan vlan-id] [interface interface]
```

**Parameters**

- **linecard slot**
  
  (REQUIRED) Enter the keyword linecard then a slot number to select the linecard for which to gather information.
show cam mac linecard (dynamic or static)

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax

```
show cam mac linecard slot port-set port-pipe [address mac-addr | dynamic | interface interface | static | vlan vlan-id]
```

Parameters

- **linecard slot** (REQUIRED) Enter the keyword linecard then a slot number to select the linecard for which to gather information.
- **port-set port-pipe** (REQUIRED) Enter the keywords port-set then a Port-Pipe number to select the Port-Pipe for which to gather information. The range is from 0 or 1.
- **address mac-addr** (OPTIONAL) Enter the keyword address then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
**dynamic**  
(Optionalal) Enter the keyword *dynamic* to display only those MAC addresses the switch dynamically learns.

**interface interface**  
(Optionalal) Enter the keyword *interface* then the interface type, slot and port information:
- For a port channel interface, enter the keywords *port-channel* then a number.
- For a 1-Gigabit Ethernet interface, enter the keyword *GigabitEthernet* then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword *TenGigabitEthernet* then the slot/port information.

**static**  
(Optionalal) Enter the keyword *static* to display only those MAC addresses specifically configured on the switch.

**vlan vlan-id**  
(Optionalal) Enter the keyword *vlan* then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

**Command Modes**
- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
8.5.1.0 | Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 | Introduced on the S4810.
7.5.1.0 | Introduced on the C-Series.
pre-6.2.1.1 | Introduced on the E-Series.

**Example**

```bash
Dell# show cam mac linecard 1 port-set 0
Port - (TableID) assignments:
  00(01) 01(01) 02(01) 03(01) 04(01) 05(01) 06(01) 07(01) 08(01) 09(01) 10(01) 11(01)
  12(01) 13(01) 14(01) 15(01) 16(01) 17(01) 18(01) 19(01) 20(01) 21(01) 22(01) 23(01)
Index Table ID VlanId Mac Address Region Interface
  0   1   0 00:01:e8:0d:b7:3b LOCAL_DA le000
  1   1   0 00:01:e8:0d:b7:3a LOCAL_DA le000
 101  0   0 00:01:e8:00:04:00 SYSTEM_STATIC 01c05
 102  0   0 01:80:00:00:00:00 SYSTEM_STATIC 01c05
 103  0   0 01:00:c:c:c:c:c:c SYSTEM_STATIC 01c01
 104  0   0 01:80:c2:00:00:02 SYSTEM_STATIC 01c02
 105  0   0 01:80:c2:00:00:0e SYSTEM_STATIC 01c01
 106  0   0 00:01:e8:0d:b7:68 SYSTEM_STATIC DROP
 107  0   0 00:01:e8:0d:b7:67 SYSTEM_STATIC DROP
 108  0   0 00:01:e8:0d:b7:66 SYSTEM_STATIC DROP
 109  0   0 00:01:e8:0d:b7:65 SYSTEM_STATIC DROP
 110  0   0 00:01:e8:0d:b7:64 SYSTEM_STATIC DROP
 111  0   0 00:01:e8:0d:b7:63 SYSTEM_STATIC DROP
 112  0   0 00:01:e8:0d:b7:62 SYSTEM_STATIC DROP
 113  0   0 00:01:e8:0d:b7:61 SYSTEM_STATIC DROP
```
show mac-address-table

Display the MAC address table.

Syntax

show mac-address-table [address mac-address | interface interface | vlan vlan-id] [aging-time] [dynamic | static] [count [vlan vlan-id] [interface interface-type [slot [/port]]]]

Parameters

- **address mac-address** (OPTIONAL) Enter the keyword address then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
- **dynamic** (OPTIONAL) Enter the keyword dynamic to display only those MAC addresses the switch dynamically learns. Optionally, you can also add one of these combinations: address/mac-address, interface/interface, or vlan vlan-id.
- **static** (OPTIONAL) Enter the keyword static to display only those MAC addresses specifically configured on the switch. Optionally, you can also add one of these combinations: address/mac-address, interface/interface, or vlan vlan-id.
- **aging-time** Enter the keyword aging-time to display only aging-time information.
- **interface interface** (OPTIONAL) Enter the keyword interface and the interface information:
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- **interface interface-type** (OPTIONAL) Instead of entering the keyword interface then the interface type, slot/port information, as above, you can enter the interface type, then just a slot number.
- **vlan vlan-id** (OPTIONAL) Enter the keyword vlan then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.
- **count** (OPTIONAL) Enter the keyword count, then optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Usage Information The following describes the show mac-address-table command shown in the following example.

### Column Heading Description

**VlanId** Displays the VLAN ID number.

**Mac Address** Displays the MAC address in nn:nn:nn:nn:nn:nn format.

**Type** Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).

**Interface** Displays the interface type and slot/port information. The following abbreviations describe the interface types:
- Po = port channel
- Gi = gigabit Ethernet
- Te = ten-gigabit Ethernet

**State** Lists if the MAC address is in use (Active) or not in use (Inactive).

### Example

```
Dell(conf)# do show mac-address-table
Codes: *N - VLT Peer Synced MAC
VlanId Mac Address Type Interface       State
2  00:00:00:00:00:01 Dynamic (N) Po 128 Active
2  00:00:00:00:00:02 Dynamic (N) Po 10  Active
2  00:00:00:00:00:03 Dynamic            Po 100 Active
2  00:00:00:00:00:04 Dynamic            Po 10  Active
```

### Usage Information

The following describes the show mac-address-table count command shown in the following example.

#### Line Beginning With Description

- **MAC Entries...** Displays the number of MAC entries learned per VLAN.
- **Dynamic Address...** Lists the number of dynamically learned MAC addresses.
Line Beginning 
With               Description
Static Address...  Lists the number of user-defined MAC addresses.
Total MAC...       Lists the total number of MAC addresses the switch uses.

Example (Count)    Dell# show mac-address-table count
MAC Entries for all vlans:
Dynamic Address Count : 110
Static Address (User-defined) Count : 0
Sticky Address Count : 0
Total Synced Mac from Peer(N): 100
Total MAC Addresses in Use: 110
Dell#

Related Commands  • show mac-address-table aging-time — display MAC aging time.

show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

Syntax            show mac-address-table aging-time [vlan vlan-id]
Parameters        vlan vlan-id (OPTIONAL) Enter the keyword vlan then the VLAN ID to display the MAC address
                   assigned to the VLAN. The range is from 1 to 4094.
Command Modes    • EXEC
                   • EXEC Privilege

Command History   This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
                   OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
| 8.3.1.0    | Added the vlan option on the E-Series.
show mac accounting destination

Display destination counters for Layer 2 traffic (available on physical interfaces only).

Syntax

show mac accounting destination [mac-address vlan vlan-id] [interface interface [mac-address vlan vlan-id] [vlan vlan-id]] [vlan vlan-id]

Parameters

mac-address (OPTIONAL) Enter the MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.

interface interface (OPTIONAL) Enter the keyword interface then the interface type, slot and port information:

• For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

vlan vlan-id (OPTIONAL) Enter the keyword vlan then the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
8.3.19.0 Introduced on the S4820T.
8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 Introduced on the S4810.
MAC Accounting information can be accessed using SNMP via the Force10 Monitor MIB. For more information about enabling SNMP, refer to the Dell Networking OS Configuration Guide.

**NOTE:** Currently, the Force10 MONITOR MIB does not return the MAC addresses in an increasing order using SNMP. As a workaround, you can use the `-C c` option in snmpwalk or snmpbulkwalk to access the Force10 MONITOR MIB. For example: `% snmpwalk -C c -v 2c -c public 133.33.33.131 enterprise.6027.3.3.3`.

**Example**

```
Dell-1# show mac accounting destination interface gigabitethernet 2/1

Destination         Out Port  VLAN  Packets  Bytes
00:44:00:00:00:02   Gi 11/1  1000  10000    5120000
00:44:00:00:00:01   Gi 11/1  1000  10000    5120000
00:22:00:00:00:00   Gi 11/1  1000  10000    5120000
00:44:00:00:00:02   Gi 11/1  2000  10000    5120000
00:44:00:00:00:01   Gi 11/1  2000  10000    5120000

Dell-1#
```

**Related Commands**

- `show mac accounting access-list` — display the MAC access list configurations and counters (if configured).

---

**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 the interface information:
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version Description

- **9.8(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.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.5.1.0** Added support for 4-port 40G line cards on E-Series.
- **8.3.7.0** Introduced on the S4810.
- **8.3.1.0** Added the `vlan` option on the E-Series.
- **7.7.1.0** Introduced on the C-Series.
- **7.5.1.0** Added support for the `violate-action` and `detail` options.
- **6.5.1.0** Added support for Port Channel.

### Example

```
Dell# show mac learning-limit
Interface  Learning  Dynamic    Static     Unknown SA
Slot/port  Limit     MAC count  MAC count  Drops
Gi 1/1     10        0          0          0
Gi 1/2     5         0          0          0
Dell#show mac learning-limit interface gigabithethernet 1/1
Interface  Learning  Dynamic    Static     Unknown SA
Slot/port  Limit     MAC count  MAC count  Drops
Gi 1/1     10        0          0          0
```

### Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

**NOTE:** For more information, refer to VLAN Stacking and VLAN-related commands, such as `portmode hybrid` in the Interfaces chapter.

#### default vlan-id

Specify a VLAN as the Default VLAN.

**Syntax**

```
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**
- Default VLAN is VLAN 1.

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
- To return VLAN 1 as the Default VLAN, use this command syntax (`default-vlan-id 1`).
- The Default VLAN contains only untagged interfaces.

**Related Commands**
- `interface vlan` — configure 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
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### 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**

```plaintext
name vlan-name
```

To remove the name from the VLAN, use the no name command.

**Parameters**

- `vlan-name`: Enter up to 32 characters as the name of the VLAN.

**Defaults**

Not configured.

**Command Modes**

INTERFACE VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>

Version | Description
--- | ---
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pref-6.2.1.1 | Introduced on the E-Series.

Usage Information
To display information about a named VLAN, enter the `show vlan` command with the `name` parameter or the `show interfaces description` command.

Related Commands
- `interface vlan` — configure a VLAN.
- `show vlan` — display the current VLAN configurations on the switch.

**show config**

Display the current configuration of the selected VLAN.

**Syntax**

```
show config
```

**Command Modes**

```
INTERFACE VLAN
```

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pref-6.2.1.1 | Introduced on the E-Series.

**Example**

```
Dell(conf-if-vl-100)# show config
!
interface Vlan 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
9.1.(0.0) Updated to support OpenFlow.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Augmented to display PVLAN data for the C-Series and S-Series and revised the output
to include the Description field to display a user-entered VLAN description.
### Version Description
- **7.6.1.0**: Introduced on the S-Series and revised the output to display Native VLAN.
- **7.5.1.0**: Introduced on the C-Series.
- **pre-6.2.1.1**: Introduced on the E-Series.

### Usage Information
The following describes the `show vlan` command shown in the following example.

<table>
<thead>
<tr>
<th>Column Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NUM</strong></td>
<td>Displays existing VLAN IDs.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Displays the word <em>Inactive</em> for inactive VLANs and the word <em>Active</em> for active VLANs.</td>
</tr>
<tr>
<td><strong>Q</strong></td>
<td>Displays G for GVRP tagged VLAN.</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>Displays the type, slot, and port information.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show vlan

Codes: * - Default VLAN, G - GVRP VLANs, P - Primary, C - Community, I - Isolated
Q: U - Untagged, T - Tagged, O - Openflow
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

NUM | Status  | Description | Q Ports |
----|---------|-------------|---------|
 1  | Inactive|             |         |
 2  | Active  |             | U Po1(Gi 1/1) T Po20(Gi 1/6), Gi 1/25 |
```

- Asterisk symbol (*) = Default VLAN
- G = GVRP VLAN
- P = primary VLAN
- C = community VLAN
- I = isolated VLAN
- O = OpenFlow

- Displays G for GVRP tagged VLAN
- M for member of a VLAN-Stack VLAN
- T for tagged interface
- U for untagged interface
- x (not capitalized x) for Dot1x untagged
- X (capitalized X) for Dot1x tagged
- o (not capitalized o) for OpenFlow untagged
- O (capitalized O) for OpenFlow tagged
- H for VSN tagged
- i (not capitalized i) for Internal untagged
- I (capitalized I) for Internal tagged
- v (not capitalized v) for VLT untagged
- V (capitalized V) for VLT tagged
3 Active T Po20(Gi 1/6) T Gi 1/7
   U Gi 1/1
4 Active U Po2(Gi 1/2) T Gi 1/7
   U Gi 1/3
5 Active T Po20(Gi 1/6) T Gi 1/7
   U Gi 1/3
6 Active U Po3(Gi 1/4) T Gi 1/7
   U Gi 1/5
7 Active T Po20(Gi 1/6) T Gi 1/7
   U Gi 1/5
P 100 Active T Po1(Gi 1/1) T Gi 1/2
C 101 Inactive T Gi 1/3
I 102 Inactive T Gi 1/4

Example (VLAN ID) Dell# show vlan id 40
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

   NUM Status Description Q Ports
   40   Active M Gi 1/47

Dell# show vlan id 41
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

   NUM Status Description Q Ports
   41   Active T Gi 1/47

Dell# show vlan id 42
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

   NUM Status Description Q Ports
   42   Active U Gi 1/47

Example (Brief) Dell# show vlan br
VLAN Name STG MAC Aging IP Address
---- ---------------------------
   1   0  1800   unassigned
   2   0  1800   2.2.2.2/24
   3   0  1800   3.3.3.2/24

Example (Name) Dell(conf)# interface vlan 222
Dell(conf-if-vi-222)# name test
Dell(conf-if-vi-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
Example (OpenFlow instance)

```
  NUM Status Description Q Ports
  * 1  Inactive
  3  Inactive
  6  Inactive
  8  Inactive
  12 Inactive
  16 Inactive

Dell(conf-if-vl-222)#
```

Related Commands

- `vlan-stack compatible` — enable the Stackable VLAN feature on the selected VLAN.
- `interface vlan` — configure a VLAN.

**tagged**

Add a Layer 2 interface to a VLAN as a tagged interface.

```
tagged interface
```

To remove a tagged interface from a VLAN, use the `no tagged interface` command.

**Syntax**

```
tagged interface
```

**Parameters**

- `interface` Enter the following keywords and the interface information:
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults**

All interfaces in Layer 2 mode are untagged.

**Command Modes**

- INTERFACE VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
### Version Description
8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.2.1.1 Introduced on the E-Series.

#### Usage Information
When you use the `no tagged` command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

#### Related Commands
- `interface vlan` — configure a VLAN.
- `untagged` — specify 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 the interface information:
  
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.

#### Defaults
Not configured.

#### Command Modes
- INTERFACE VLAN

#### Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

#### Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
### Version Description

- **9.2(1.0)**
  - Introduced on the Z9500.
- **9.0.2.0**
  - Introduced on the S6000.
- **8.3.19.0**
  - Introduced on the S4820T.
- **8.3.11.1**
  - Introduced on the Z9000.
- **8.5.1.0**
  - Added support for 4-port 40G line cards on the E-Series.
- **8.3.7.0**
  - Introduced on the S4810.
- **7.6.1.0**
  - Introduced on the S-Series.
- **7.5.1.0**
  - Introduced on the C-Series.
- **pre-6.2.1.1**
  - Introduced on the E-Series.

#### Usage Information

When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If the `track ip` command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and the Layer 2 traffic, is not affected by the `track ip` command configuration.

#### Related Commands

- **interface vlan** — configure a VLAN.
- **tagged** — specify 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 the interface information:
    - For a port channel interface, enter the keywords `port-channel` then a number.
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

### Defaults

All interfaces in Layer 2 mode are untagged.

### Command Modes

`INTERFACE VLAN`
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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 — configure a VLAN.
- tagged — specify which interfaces in a VLAN are tagged.

Far-End Failure Detection (FEFD)

The Dell Networking operating software supports far-end failure detection (FEFD) on the Ethernet interfaces of the S3048–ON platform. The FEFD feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- During an RPM failover, FEFD is operationally disabled for approximately 8 to 10 seconds.
- By default, FEFD is disabled.

debug fefd

Enable debugging of FEFD.

Syntax
```
debug fefd {events | packets} [interface]
```

To disable debugging of FEFD, use the no debug fefd {events | packets} [interface] command.
Parameters

- **events**
  - Enter the keyword `events` to enable debugging of FEFD state changes.

- **packets**
  - Enter the keyword `packets` to enable debugging of FEFD to view information on packets sent and received.

- **interface**
  - (OPTIONAL) Enter the following keywords and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Command Modes

**EXEC Privilege**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Legacy E-Series command.

Related Commands

- `fefd` — enable far-end failure detection on an interface.
- `fefd reset` — enable FEFD globally on the system.

---

**fefd**

Enable Far-End Failure Detection on an interface, set the FEFD interval, or select the FEFD mode.

**Syntax**

```plaintext
fefd {disable|interval|mode {aggressive|normal}}
```

**Parameters**

- **disable**
  - Enter the keyword `disable` to disable FEFD for the specified interface.

- **interval**
  - Enter the keyword `interval`, followed by a value to specify the FEFD interval in seconds. Range is from 3 to 300. Default is 15.

- **mode**
  - Enter the keyword `mode` followed by the mode type to specify the FEFD mode.
    - **normal**: Change the link state to “unknown” when a far-end failure is detected by the software on that interface. When the interface is placed in an “unknown” state, the software brings down the line protocol.
    - **aggressive**: Change the link state to “error-disabled” when a far-end failure is detected by the software on that interface. When an interface is placed in an “error-
disabled" state, you must enter the `fefd reset` command to reset the interface state. Range is normal or aggressive. Default is normal.

Defaults
Disabled.

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information
When you enter no fefd for an interface and fefd-global, FEFD is enabled on the interface because the no fefd command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the fefd reset command.

Related Commands
- `fefd disable` — disable far-end failure detection on an interface.
- `fefd reset` — enable FEFD globally on the system.
- `fefd mode` — change FEFD mode on an interface.

**fefd disable**

Disable FEFD on an interface only. This command overrides the `fefd reset` command for the interface.

Syntax
```plaintext
fefd disable
```

To re-enable FEFD on an interface, use the `no fefd disable` command.

Defaults
Not configured.

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
8.3(19.0) | Introduced on the S4820T.
8.3(11.1) | Introduced on the Z9000.
8.3(7.0) | Introduced on the S4810.

**Legacy E-Series command.**

**Usage Information**
FEFD disable command on the interface prevents the interface from running FEFD when FEFD is enabled globally.

**Related Commands**
- `fefd reset` — clear an interface in Err-disabled state. It doesn’t work until the interface is in err-disabled state.
- `fefd mode` — change FEFD mode on an interface.

---

**fefd interval**

Set an interval between control packets.

**Syntax**

```
fefd interval seconds
```

To return to the default value, use the `no fefd interval` command.

**Parameters**

- `seconds` Enter a number as the time between FEFD control packets. The range is from 3 to 255 seconds. The default is **15 seconds**.

**Defaults**

15 seconds

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
8.3(19.0) | Introduced on the S4820T.
8.3(11.1) | Introduced on the Z9000.
8.3(7.0) | Introduced on the S4810.

**Legacy E-Series command.**

**Usage Information**
You can set up the interval between control packets using the `fefd interval` command.
Related Commands

- `fefd` — enable far-end failure detection.

**fefd mode**

Change the FEFD mode on an interface.

**Syntax**

`fefd mode {normal | aggressive}`

To return the FEFD mode to the default of normal, use the `no fefd mode` command.

**Parameters**

- `normal` (OPTIONAL) Enter the keyword `normal` to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol.

- `aggressive` (OPTIONAL) Enter the keyword `aggressive` to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, enter the `fefd reset` command to reset the interface state.

**Defaults**

Normal

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Legacy E-Series command.

**Related Commands**

- `fefd` — enable far-end failure detection.

**fefd reset**

Reset all interfaces or a single interface that was in “error-disabled” mode.

**Syntax**

`fefd reset [interface]`
Parameters

`interface` (OPTIONAL) Enter the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>Legacy E-Series command.</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands

- `fefd` — enable far-end failure detection.

**`fefd-global interval`**

Configure an interval between FEFD control packets.

**Syntax**

`fefd-global interval seconds`

To return to the default value, use the `no fefd-global interval` command.

**Parameters**

- `seconds` Enter a number as the time between FEFD control packets. The range is from 3 to 300 seconds. The default is **15 seconds**.

**Defaults**

**15 seconds**

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
8.3(19.0) | Introduced on the S4820T.
8.3(11.1) | Introduced on the Z9000.
8.3(7.0) | Introduced on the S4810.

Legacy E-Series command.

**Related Commands**
- **fefd** — enable far-end failure detection.
- **fefd-global** — enable FEFD globally on the system.

## fefd-global

Enable FEFD globally on the system.

**Syntax**
```
fefd-global [interval seconds][mode {normal | aggressive}]
```

To disable FEFD globally, use the `no fefd-global [mode {normal | aggressive}]` command.

**Parameters**
- **interval seconds**
  - Enter the keyword `interval` followed by the number of seconds to wait between FEFD control packets. Range is from 3 to 300 seconds. Default is 15 seconds.
- **normal**
  - (OPTIONAL) Enter the keywords `mode normal` to change the link state to “unknown” when a far-end failure the software detects on that interface. When the interface is placed in “unknown” state, the software brings down the line protocol. The default is Normal mode.
- **aggressive**
  - (OPTIONAL) Enter the keywords `mode aggressive` to change the link state to “error-disabled” when a far-end failure the software detects on that interface. When an interface is placed in “error-disabled” state, enter the `fefd reset` command to reset the interface state.

**Defaults**
- Disabled.

**Command Modes**
- CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
Version Description
9.7(0.0)    Introduced on the S6000-ON.
9.2(1.0)    Introduced on the Z9500.
9.0.2.0     Introduced on the S6000.
8.3.19.0    Introduced on the S4820T.
8.3.11.1    Introduced on the Z9000.
8.3.12.0    Introduced on the S4810.

Legacy E-Series
command.

Usage Information
If you enter only the `fefd-global` syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (`no fefd-global`), the system does not remove the FEFD interface configuration.

Related Commands
- `fefd` — enable far-end failure detection.
- `fefd-global interval` — configure an interval between FEFD control packets.
- `show fefd` — display the FEFD command output.

show fefd

View FEFD status globally or on a specific interface.

Syntax
```
show fefd [interface]
```

Parameters
- `interface` (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(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.
Version  Description
8.3.19.0  Introduced on the S4820T.
8.3.11.1  Introduced on the Z9000.
8.3.12.0  Introduced on the S4810.

Legacy E-Series command.

Usage Information The following describes the show fefd command shown in the following example.

Field  Description
Interface  Displays the interfaces type and number.
Mode  Displays the mode (aggressive or normal) or NA if the interface contains fefd reset in its configuration.
Interval  Displays the interval between FEFD packets.
State  Displays the state of the interface and can be one of the following:
   • bi-directional (interface is up, connected and hearing neighbor’s echoes).
   • err-disabled (only found when FEFD mode is aggressive and when the interface has not hearing its neighbor’s echoes for three times the message interval. To reset an interface in this state, use the fefd reset command.)
   • unknown (only found when FEFD mode is normal.
   • locally disabled (interface contains the fefd reset command in its configuration).
   • Admin Shutdown (interface is disabled with the shutdown command).

Example Dell# show fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>MODE</th>
<th>INTERVAL</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi 5/1</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/2</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/3</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/4</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/5</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/6</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/7</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/8</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/9</td>
<td>Aggressive</td>
<td>10</td>
<td>Admin Shutdown</td>
</tr>
<tr>
<td>Gi 5/10</td>
<td>NA</td>
<td>NA</td>
<td>Locally disabled</td>
</tr>
<tr>
<td>Gi 5/11</td>
<td>Aggressive</td>
<td>10</td>
<td>Err-disabled</td>
</tr>
</tbody>
</table>

Dell#

Related Commands
• fefd — enable far-end failure detection.
• fefd disable — disable FEFD on an interface only.
• fefd-global — enable FEFD globally on the system.
• fefd reset — reset all interfaces or a single interface that was in “error-disabled” mode.
Link Layer Discovery Protocol (LLDP)

The link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.
LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating software implementation of LLDP is based on IEEE standard 801.1ab.

The Dell Networking OS supports the basic LLDP commands on S3048–ON platform.
The starting point for using LLDP is invoking LLDP with the protocol lldp command in either CONFIGURATION or INTERFACE mode.
The information LLDP distributes is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

Topics:
• LLPD Commands
• LLDP-MED Commands

LLPD Commands

The following are LLDP commands.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

Syntax
advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}

To remove advertised dot1-tlv, use the no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name} command.

Parameters
port-protocol-vlan-id
Enter the keywords port-protocol-vlan-id to advertise the port protocol VLAN identification TLV.
port-vlan-id
Enter the keywords port-vlan-id to advertise the port VLAN identification TLV.
vlan-name
Enter the keywords vlan-name to advertise the vlan-name TLV. This keyword is only supported on the C-Series and S-Series.

Defaults
Disabled.

Command Modes
CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)
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 TLV.

Defaults

None

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series. Added the vlan-name option.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- protocol lldp (Configuration) — enable LLDP globally.
- debug lldp interface — debug LLDP.
- show lldp neighbors — display the LLDP neighbors.
advertise management-tlv

Advertise management TLVs (Type, Length, Value).

Syntax
advertise management-tlv {management-address | system-capabilities | system-description | system-name}

To remove advertised management TLVs, use the no advertise management-tlv {management-address | system-capabilities | system-description | system-name} command.

Parameters
- **management-address**: Enter the keyword management-address to advertise the management IP address TLVs to the LLDP peer.
- **system-capabilities**: Enter the keywords system-capabilities to advertise the system capabilities TLVs to the LLDP peer.
- **system-description**: Enter the keywords system-description to advertise the system description TLVs to the LLDP peer.
- **system-name**: Enter the keywords system-name to advertise the system name TLVs to the LLDP peer.

Defaults
None

Command Modes
CONFIGURATION (conf-lldp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
| 91.0(0.0) | Modified to support management-address parameter.
advertise management-tlv (Interface)

Advertise management type, length, values (TLVs) to the specified interface.

Syntax
advertise management-tlv {management-address | system-capabilities | system-description | system-name}

To remove advertised management TLVs, use the no advertise management-tlv {management-address | system-capabilities | system-description | system-name} command.

Parameters
management-address Enter the keywords management-address to advertise the management IP address TLVs to the specified interface.

system-capabilities Enter the keywords system-capabilities to advertise the system capabilities TLVs to the specified interface.

system-description Enter the keywords system-description to advertise the system description TLVs to the specified interface.

system-name Enter the keywords system-name to advertise the system name TLVs to the specified interface.

Defaults
None

Command Modes
INTERFACE (conf-interface-lldp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
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 Z9000 and S4810.
8.3.19.0 Introduced on the S4820T.
clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax

```
clear lldp counters [interface interface]
```

Parameters

- **interface interface** (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Defaults

None

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
**clear lldp neighbors**

Clear LLDP neighbor information for all interfaces or a specific interface.

**Syntax**

```
clear lldp neighbors [interface interface]  
```  

**Parameters**

- **interface interface** (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword **GigabitEthernet** then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** then the slot/port information.

**Defaults**

None

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
debug lldp interface

To display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets, enable LLDP debugging.

Syntax

debug lldp interface {interface | all} {events | packet {brief | detail} {tx | rx | both}}

To disable debugging, use the no debug lldp [interface {interface | all} {events} {packet {brief | detail} {tx | rx | both}}] command.

Parameters

interface interface Enter the following keywords and slot/port or number information:

  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

all Enter the keyword all to display information on all interfaces.

events Enter the keyword events to display major events such as timer events.

packet Enter the keyword packet to display information regarding packets coming in or going out.

brief Enter the keyword brief to display brief packet information.

detail Enter the keyword detail to display detailed packet information.

rx Enter the keyword rx to display receive-only packet information.

both Enter the keyword both to display both receive and transmit packet information.

Defaults None

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.5.1.0 Added support for 4-port 40G line cards on the E-Series.
Enable or disable LLDP.

Syntax
disable
To enable LLDP, use the no disable command.

Defaults
Enabled — no disable.

Command Modes
CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.7.1.0 Introduced on the S-Series.
7.6.1.0 Introduced on the C-Series.
7.4.1.0 Introduced on the E-Series.

Related Commands
- protocol lldp (Configuration) — enable LLDP globally.
- debug lldp interface — debug LLDP.
- show lldp neighbors — display the LLDP neighbors.
**hello**

Configure the rate at which the LLDP control packets are sent to its peer.

**Syntax**

```
hello seconds
```

To revert to the default, use the `no hello seconds` command.

**Parameters**

- `seconds` Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is from 5 to 180 seconds. The default is **30 seconds**.

**Defaults**

**30 seconds**

**Command Modes**

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**management-interface**

Enable and configure LLDP protocol parameters on the management interface.

**Syntax**

```
management-interface
```

To remove LLDP configuration on a management interface, use the `no management-interface` command.
**Command Modes**

LLDP (conf-lldp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000 and S4810.</td>
</tr>
</tbody>
</table>

**Usage Information**

To enable LLDP on the management interface, use the `no disable` command in LLDP-MANAGEMENT-INTERFACE mode (conf-lldp-mgmtIf).

---

**mode**

To receive or transmit, set LLDP.

**Syntax**

`mode {tx | rx}`

To return to the default, use the `no mode` command.

**Parameters**

- `tx`: Enter the keyword `tx` to set the mode to transmit.
- `rx`: Enter the keyword `rx` to set the mode to receive.

**Defaults**

Both `transmit` and `receive`.

**Command Modes**

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-interface-lldp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
multiplier

Set the multiple of the hello timer before LLDP declares the interface dead.

Syntax

multiplier number

To return to the default, use the no multiplier command.

Parameters

- **integer**
  - Enter the number of consecutive misses before the LLDP declares the interface dead.
  - The range is from 2 to 10.

Defaults

4

Command Modes

- CONFIGURATION (conf-lldp)
- INTERFACE (conf-if-interface-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
**protocol lldp (Configuration)**

Enable the 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)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**protocol lldp (Interface)**

Enter the LLDP protocol in INTERFACE mode.

Syntax

```
[no] protocol lldp
```

To return to the global LLDP configuration mode, use the `no protocol lldp` command from Interface mode.

Defaults

LLDP is not enabled on the interface.

Command Modes

INTERFACE (conf-if-interface-lldp)
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
Before LLDP can be configured on an interface, it must be enabled globally from CONFIGURATION mode. This command places you in LLDP mode on the interface; it does not enable the protocol.

When you enter the LLDP protocol in the Interface context, it overrides global configurations. When you execute the no protocol lldp from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

show lldp neighbors
Display LLDP neighbor information for all interfaces or a specified interface.

Syntax
show lldp neighbors [interface interface] [detail]

Parameters
interface interface (OPTIONAL) Enter the following keywords and the interface information:
- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
detail (OPTIONAL) Enter the keyword detail to display all the TLV information, remote management IP addresses, timers, and LLDP tx and rx counters.

Defaults
None

Command Modes
EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Modified output of detail parameter to display remote management IP addresses.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

Omitting the keyword detail displays only the remote chassis ID, Port ID, and Dead Interval.

### Example

```
R1(conf-if-gi-1/31)# do show lldp neighbors
Loc PortID Rem Host Name       Rem Port Id Rem Chassis Id
Gi 1/21    R2   GigabitEthernet 2/11  00:01:e8:06:95:3e
Gi 1/31    R3   GigabitEthernet 3/11  00:01:e8:09:c2:4a
```

### show lldp statistics

Display the LLDP statistical information.

#### Syntax

```
show lldp statistics
```

#### Defaults

None

#### Command Modes

EXEC Privilege

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
**Example**

Dell# show lldp statistics
Total number of neighbors: 300
Last table change time   :   Mon Oct 02 16:00:52 2006
Number of Table Inserts  :   1621
Number of Table Deletes  :   200
Number of Table Drops    :   0
Number of Table Age Outs :   400
Dell#

**show management-interface**

Display LLDP management interface configuration information.

**Syntax**

```
show management-interface
```

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Introduced on the Z9000 and S4810.</td>
</tr>
</tbody>
</table>

**show running-config lldp**

Display the current global LLDP configuration.

**Syntax**

```
show running-config lldp
```
Defaults
None

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S8420T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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.

Dell Networking OS 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
- identify physical location
- identify network policy
advertise med guest-voice

To advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support
interactive voice services, configure the system.

Syntax

advertise med guest-voice {vlan-id layer2_priority DSCP_value} | (priority-tagged number)

To return to the default, use the no advertise med guest-voice {vlan-id layer2_priority DSCP_value} | (priority-tagged number) command.

Parameters

- **vlan-id**: Enter the VLAN ID. The range is from 1 to 4094.
- **layer2_priority**: Enter the Layer 2 priority. The range is from 0 to 7.
- **DSCP_value**: Enter the DSCP value. The range is from 0 to 63.
- **priority-tagged number**: Enter the keywords priority-tagged, the Layer 2 priority, and then the DSCP value.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

-  `protocol lldp (Configuration)` — enable LLDP globally.
-  `debug lldp interface` — debug LLDP.
-  `show lldp neighbors` — display the LLDP neighbors.
advertise med guest-voice-signaling

To advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data, configure the system.

Syntax
advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters
- **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, the Layer 2 priority, and then the DSCP value.

Defaults
- Unconfigured.

Command Modes
- CONFIGURATION (conf-lldp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands
- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
advertise med location-identification

To advertise a location identifier, configure the system.

Syntax

advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}

To return to the default, use the no advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value} command.

Parameters

- coordinate-based value
  - Enter the keywords coordinate-based then the coordinated based location in hexadecimal value of 16 bytes.
- civic-based value
  - Enter the keywords civic-based then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
- ecs-elin value
  - Enter the keywords ecs-elin then the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is from 10 to 25 characters.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

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.
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)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.

Related Commands

debug lldp interface — debugs LLDP.
show lldp neighbors — displays the LLDP neighbors.
advertise med softphone-voice

To advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone, configure the system.

Syntax
advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- `vlan-id` Enter the VLAN ID. The range is from 1 to 4094.
- `layer2_priority` Enter the Layer 2 priority. 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, the Layer 2 priority, and then the DSCP value.

Defaults
Unconfigured.

Command Modes
CONFIGURATION (conf-lldp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.71.0 | Introduced on the S-Series.
7.61.0 | Introduced on the C-Series and E-Series.

Related Commands
- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
advertise med streaming-video

To advertise streaming video services for broadcast or multicast-based video, configure the system. This command does not include video applications that rely on TCP buffering.

Syntax

advertise med streaming-video {vlan-id layer2_priority DSCP_value} | {priority-tagged number}

To return to the default, use the no advertise med streaming-video {vlan-id layer2_priority DSCP_value} | {priority-tagged number} command.

Parameters

- **vlan-id**
  - Enter the VLAN ID. The range is from 1 to 4094.
- **layer2_priority**
  - Enter the Layer 2 priority. 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, the Layer 2 priority, and then the DSCP value.

Defaults

Unconfigured.

Command Modes

- CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- debug lldp interface — debug LLDP.
- show lldp neighbors — display the LLDP neighbors.
advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

Syntax

```plaintext
advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

- **vlan-id**: Enter the VLAN ID. The range is from 1 to 4094.
- **layer2_priority**: Enter the Layer 2 priority. 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`, the Layer 2 priority, and then the DSCP value.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
advertise med video-signaling

To advertise video control packets that use a separate network policy than video data, configure the system.

**Syntax**

```
advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

**Parameters**

- **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`, the Layer 2 priority, and then the DSCP value.

**Defaults**

Unconfigured.

**Command Modes**

CONFIGURATION (conf-lldp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

Syntax

```plaintext
advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

- **vlan-id**
  - Enter the VLAN ID. The range is from 1 to 4094.
- **layer2_priority**
  - Enter the Layer 2 priority. 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`, the Layer 2 priority, and then the DSCP value.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-ldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

Syntax

```
advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}
```

To return to the default, use the `no advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

- **vlan-id**: Enter the VLAN ID. The range is from 1 to 4094.
- **layer2_priority**: Enter the Layer 2 priority. 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`, the Layer 2 priority, and then the DSCP value.

Defaults

Unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- `debug lldp interface` — debug LLDP.
- `show lldp neighbors` — display the LLDP neighbors.
Microsoft Network Load Balancing

Network load balancing (NLB) is a clustering functionality that is implemented by Microsoft on Windows 2000 Server and Windows Server 2003 operating systems. Microsoft NLB clustering allows multiple servers running Microsoft Windows to be represented by one MAC and one IP address to provide transparent failover and load-balancing. The Dell Networking OS does not recognize server clusters by default; you must configure NLB functionality on a switch to support server clusters. The maximum NLB entry limit from 8 to 11 is increased and support for more CAM-ACL to increase.

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` Enter a vlan port to where L2 multicast MAC traffic is forwarded.

1. **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.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- `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 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a Management interface, enter the keyword `managementethernet` followed by slot/port numbers.
- For a Port Channel interface, enter the keywords `port-channel` followed by a number.
- 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.

```
vlan vlan-id
```
Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for multicast MAC address on the MXL platform.</td>
</tr>
</tbody>
</table>

**Example (Multicast)**
```
mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output-range gi 1/2,gi 1/3
```

### ip vlan-flooding

Enable unicast data traffic flooding on VLAN member ports.

**Syntax**
```
ip vlan-flooding
```
To disable, use the `no ip vlan-flooding` command.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL platforms.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Information**
By default this command is disabled. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.
Multicast Source Discovery Protocol (MSDP)

Multicast source discovery protocol (MSDP) connects multiple PIM sparse-mode (PIM-SM) domains together. MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

The Dell Networking OS supports MSDP commands on the S3048-ON platform.

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
clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

Syntax

```
clear ip msdp sa-cache [group-address | rejected-sa | local]
```

Parameters

- **group-address**: Enter the group IP address in dotted decimal format (A.B.C.D.).
- **rejected-sa**: Enter the keywords rejected-sa to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
- **local**: Enter the keyword local to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults

Without any options, this command clears the entire source-active cache.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
### clear ip msdp statistic

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

**Syntax**

```
clear ip msdp statistic peer peer-address
```

**Parameters**

- **peer**
  - Enter the keyword `peer` to clear the MSDP peer entries.
- **peer-address**
  - Enter the IP address of the MSDP peer.

**Defaults**

Without any options, this command clears the entire source-active cache.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added the local option.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the rejected-sa option.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
debug ip msdp

Turn on MSDP debugging.

Syntax
debug ip msdp {event peer address | packet peer address | pim}
To turn debugging off, use the no debug ip msdp {event peer address | packet peer address | pim} command.

Parameters
- **event peer address**: Enter the keyword `event` then the peer address in a dotted decimal format (A.B.C.D).
- **packet peer address**: Enter the keyword `packet` then the peer address in a dotted decimal format (A.B.C.D).
- **pim**: Enter the keyword `pim` to debug advertisement from PIM.

Defaults
Not configured.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

ip msdp cache-rejected-sa

Enable an MSDP cache for the rejected source-active entries.

Syntax
ip msdp cache-rejected-sa {number}
To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {number}` command then the `ip msdp cache-rejected-sa {number}` command.

**Parameters**

- `number`  
  Enter the number of rejected SA entries to cache. The range is from 0 to 32766.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Related Commands**

- `show ip msdp sa-cache rejected-sa` — display 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**

```plaintext
ip msdp default-peer peer address [list name]
```

To remove the default peer, use the `no ip msdp default-peer {peer address} list name` command.

**Parameters**

- `peer address`  
  Enter the peer address in a dotted decimal format (A.B.C.D.)

- `list name`  
  Enter the keywords `list name` and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION
### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added the list option and removed the prefix-list option.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

### 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
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

- **name**: Enter a string of up to 16 characters long for as the mesh group name.
- **peer address**: Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
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**: Enter the keywords `connect-source` then one of the interfaces and slot/port or number information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- **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 100000.

Defaults

See Parameters.

Command Modes

**CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which the ACL denies time out and are not refreshed. Until they time out, they continue to reside in the MSDP SA cache.

**Syntax**

```
ip msdp redistribute [list acl-name]
```

**Parameters**

- `list acl-name` Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
Modifications to the ACL do not have an immediate effect on the sa-cache.

To apply the redistribute filter to entries already present in the SA cache, use the `clear ip msdp sa-cache local` command.

**ip msdp sa-filter**

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

**Syntax**

```plaintext
ip msdp sa-filter {in | out} peer-address list [access-list name]
```

Remove this configuration using the `no ip msdp sa-filter {in | out} peer address list [access-list name]` command.

**Parameters**

- **in**: Enter the keyword `in` to enable incoming SA filtering.
- **out**: Enter the keyword `out` to enable outgoing SA filtering.
- **peer-address**: Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
- **access-list name**: Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

**Defaults**

Not configured.

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
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 1 to 500000.

Defaults

50000

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
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.5.1.0 Introduced on the E-Series.

Usage Information

Dell Networking OS counts the SA messages originated by itself and those messages received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in Dell Networking OS continue to be accepted. To enforce the limit in such situation, use the clear ip msdp sa-cache command.

Related Commands

- ip msdp peer — configure the MSDP peer.
- clear ip msdp peer — clear the MSDP peer.
- show ip msdp — display 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**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
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>
show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

Syntax

show ip msdp sa-cache rejected-sa

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(10) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.
**Version** | **Description**
---|---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.1 | Introduced on the S4810.
7.4.1.0 | Introduced.

**Example**

```bash
Dell# show ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache 200 rejected SAs received, cache-size 1000
MIB Time UpTime GroupAddr SourceAddr RPAddr LearnedFrom Reason
00:00:13 225.1.2.1 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.2 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.3 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.4 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.5 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.6 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.7 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.8 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.9 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.10 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.12 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.13 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.14 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.15 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.16 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.17 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.18 10.1.1.4 110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.19 10.1.1.3 110.1.1.1 13.1.1.2 Rpf-Fail
```
Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking OS, conforms to IEEE 802.1s. This command supports the Dell Networking S3048-ON platform.

Topics:
- debug spanning-tree mstp
- disable
- forward-delay
- hello-time
- max-age
- msti
- name
- protocol spanning-tree mstp
- revision
- show config
- show spanning-tree mst configuration
- show spanning-tree msti
- spanning-tree
- spanning-tree msti
- 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]
```

To disable debugging, enter `no debug spanning-tree mstp`

Parameters

- **all**
  (OPTIONAL) Enter the keyword all to debug all spanning tree operations.

- **bpdu interface**
  (OPTIONAL) Enter the keyword bpdu to debug bridge protocol data units (BPDU).

- **{in | out}**
  (OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following:

  - For a port channel interface, enter the keywords port-channel then a number.
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Optionally, enter an in or out parameter with the optional interface:

- For Receive, enter the keyword in.
- For Transmit, enter the keyword out.

**events**

(Optional) Enter the keyword `events` to debug MSTP events.

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>EXEC Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command History</strong></td>
<td>This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# debug spanning-tree mstp bpdu gigabitethernet 2/1 ?
in Receive (in)
out Transmit (out)
```

disable

Globally disable the multiple spanning tree protocol on the switch.

**Syntax**

disable

To enable MSTP, enter the no disable command.

**Defaults**

Disabled.

**Command Modes**

MULTIPLE SPANNING TREE
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

### Related Commands

- `protocol spanning-tree mstp` — enter MULTIPLE SPANNING TREE mode.

### forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

#### Syntax

```
forward-delay seconds
```

To return to the default setting, use the `no forward-delay` command.

#### Parameters

- `seconds`: Enter the number of seconds the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State. The range is from 4 to 30. The default is 15 seconds.

#### Defaults

15 seconds

#### Command Modes

MULTIPLE SPANNING TREE

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `max-age` — change the wait time before MSTP refreshes protocol configuration information.
- `hello-time` — change the time interval between bridge protocol data units (BPDUs).

### hello-time

Set the time interval between generation of MSTB bridge protocol data units (BPDUs).

**Syntax**

```
hello-time seconds
```

To return to the default value, use the `no hello-time` command.

**Parameters**

- `seconds` Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

**Defaults**

**2 seconds**

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.5.1.0 | Introduced.

Related Commands
- `forward-delay` — amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
- `max-age` — change 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 Dell Networking OS waits before refreshing configuration information. The range is from 6 to 40. The default is 20 seconds.

**Defaults**
- 20 seconds

**Command Modes**
- MULTIPLE SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>
Related Commands

- **forward-delay** — amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
- **hello-time** — change the time interval between BPDUs.

---

**msti**

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

**Syntax**

```plaintext
msti instance {vlan range | bridge-priority priority}
```

To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

**Parameters**

- **msti instance**
  - Enter the MSTP instance. The range is from zero (0) to 63.
- **vlan range**
  - Enter the keyword `vlan` then the identifier range value. The range is from 1 to 4094.
- **bridge-priority priority**
  - Enter the keywords `bridge-priority` then a value in increments of 4096 as the bridge priority. The range is from zero (0) to 61440.
  - Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

**Defaults**

default bridge-priority is **32768**.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>
Usage Information

By default, all VLANs are mapped to MST instance zero (0) unless you use the vlan range command to map it to a non-zero instance.

**name**

The name you assign to the multiple spanning tree region.

**Syntax**

name region-name

To remove the region name, use the no name command.

**Parameters**

- **region-name**
  
Enter the MST region name. The range is 32 character limit.

**Defaults**

No default name.

**Command Modes**

MULTIPLE SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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** — map the VLAN(s) to an MST instance.
- **revision** — assign the revision number to the MST configuration.
protocol spanning-tree mstp

To enable and configure the multiple spanning tree group, enter MULTIPLE SPANNING TREE mode.

Syntax

    protocol spanning-tree mstp

To disable the multiple spanning tree group, use the no protocol spanning-tree mstp command.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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 — disable 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

For two MSTP switches to be within the same MST region, the switches must share the same revision number.

Related Commands

- `msti` — map the VLAN(s) to an MST instance.
- `name` — assign 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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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**

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4(2.1)</td>
<td>Support for the optional keyword guard was added on the C-Series, S-Series, and E-Series.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.4(1.0)</td>
<td>Expanded to display the port error disable state (EDS) loopback BPDU inconsistency causes.</td>
</tr>
</tbody>
</table>

**Usage Information**
Enable the multiple spanning tree protocol prior to using this command.

**Example**
```
Dell# show spanning-tree msti 10
MSTI 10 VLANs mapped 101-105

Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occurred 3058087

Port 82 (GigabitEthernet 2/1) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (GigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
The port is not in the portfast mode

Port 89 (GigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
```
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode

The bold line shows the loopback BPDU inconsistency (LBK_INC).

Example (EDS and LBK)

Dell# show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0

Interface                            Designated
Name    PortID   Prio Cost Sts Cost Bridge ID      PortID
----------------------------------------------------------
Gi 1/1  128.257  128  20000 EDS 0 32768 0001.e801.6aa8 128.257

Interface
Name  Role  PortID Prio Cost Sts Cost Link-type Edge Boundary
----------------------------------------------------------
Gi 1/1 ErrDis 128.257  128 20000 EDS 0 P2P       No   No

Dell# show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occured 00:00:15 ago on Gi 1/1

Port 257 (GigabitEthernet 1/1) is LBK INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode

Usage Information
The following describes the show spanning-tree msti 5 guard command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>MSTP interface.</td>
</tr>
<tr>
<td>Instance</td>
<td>MSTP instance.</td>
</tr>
<tr>
<td>Sts</td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).</td>
</tr>
<tr>
<td>Guard Type</td>
<td>Type of STP guard configured (Root, Loop, or BPDU guard).</td>
</tr>
</tbody>
</table>

Example (Guard)

Dell# show spanning-tree msti 5 guard
Interface
Name    Instance Sts Guard    type
------------------------------------
Gi 1/1  5         INCON(Root)  Rootguard

952 | Multiple Spanning Tree Protocol (MSTP)
spanning-tree

Enable the multiple spanning tree protocol on the interface.

Syntax

```
spanning-tree
```

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

- **spanning-tree**
  
Enter the keywords `spanning-tree` to enable the MSTP on the interface.

Defaults

Enable.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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:
  - 100 Mb/s Ethernet interface = 200000
  - 1-Gigabit Ethernet interface = 20000
  - 10-Gigabit Ethernet interface = 2000
  - Port Channel interface with one 100 Mb/s Ethernet = 200000
  - Port Channel interface with one 1 Gb Ethernet = 20000
  - Port Channel interface with one 10 Gigabit Ethernet = 2000
  - Port Channel with two 1 Gb Ethernet = 18000
  - 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant [Dell Networking OS Command Line Reference Guide](https://www.dell.com/support/home). This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
**tc-flush-standard**

Enable the MAC address flushing after receiving every topology change notification.

**Syntax**

```
tc-flush-standard
```

To disable, use the `no tc-flush-standard` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, Dell Networking OS implements an optimized flush mechanism for MSTP. This mechanism helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this knob command can be turned on to enable flushing MAC addresses after receiving every topology change notification.
Multicast

The multicast commands are supported by Dell Networking OS on all S3048-ON platform.

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 [vrf vrf-name] {group-address [source-address] | * | snooping}

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

group-address  Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.

[source-address]  

*  Enter * to clear all multicast routes.

snooping  Enter the keyword snooping to delete multicast snooping route table entries.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

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.

9.2.(0.0)  Added support for keyword snooping on the Z9000, S4810, and S4820T.

9.0.2.0  Introduced on the S6000.

8.3.19.0  Introduced on the S4820T.
### ip mroute

Assign a static mroute.

**Syntax**

```plaintext
ip mroute [vrf vrf-name] destination mask {ip-address | null 0| {{bgp | ospf} process-id | isis | rip | static} {ip-address | tag | null 0}} [distance]
```

To delete a specific static mroute, use the `no ip mroute [vrf vrf-name] 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 [vrf vrf-name]destination mask` command.

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to assign a static mroute to that VRF.
  
  | NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

- **destination**
  
  Enter the IP address in dotted decimal format of the destination device.

- **mask**
  
  Enter the mask in slash prefix format (`/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.
ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Syntax

ip multicast-limit [vrf vrf-name] limit

Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to limit the number of multicast on the VRF.
- **limit** Enter the desired maximum number of multicast entries on the system. The S-Series range is from 1 to 16000.

Defaults

The S-Series default is 4000.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Related Commands

- show ip mroute — display the routing table.

---

## ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

Syntax

```
ip multicast-limit [vrf vrf-name] limit
```

Parameters

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to limit the number of multicast on the VRF.
- **limit** Enter the desired maximum number of multicast entries on the system. The S-Series range is from 1 to 16000.

Defaults

The S-Series default is 4000.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>

Related Commands

- show ip mroute — display the routing table.
Usage Information

This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile. To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

Related Commands

- `show ip igmp groups` — display the IGMP groups.

ip multicast-routing

Enable IP multicast forwarding.

Syntax

```
ip multicast-routing [vrf vrf-name]
```

To disable multicast forwarding, use the `no ip multicast-routing [vrf vrf-name]` command.

Defaults

Disabled.

Parameters

```
vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable IP multicast forwarding on that VRF.
```

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.1 Introduced on the S4810.
### Version Description

| E-Series legacy command |

**Usage Information**

After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

**Related Commands**

- `ip pim sparse-mode` — enable IGMP and PIM on an interface.

### show ip mroute

View the multicast routing table.

**Syntax**

```
show ip mroute [vrf vrf-name] [static | group-address [source-address] | count | snooping [vlan vlan-id] [group-address [source-address]] | summary | vlt [group-address [source-address] | count]
```

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.

  > **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- **static** (OPTIONAL) Enter the keyword `static` to view static multicast routes.

- **group-address** (OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.

- **count** (OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.

- **snooping [vlan vlan-id] [group-address [source-address]]**

  Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers.

  Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094.

  Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.

- **summary** (OPTIONAL) Enter the keyword `summary` to view a summary of all routes.

- **vlt** (OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

**Command Modes**

- EXEC
• EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2.(0.0)</td>
<td>Added support for keyword vlt to the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>8.4.1.1</td>
<td>Support for the keyword snooping and the optional vlan vlan-id,group-</td>
</tr>
<tr>
<td></td>
<td>address, and source-address parameters were added on E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Example (Static) Dell# show ip mroute static
Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23

Example (Snooping) Dell# show ip mroute snooping
IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
Incoming vlan: Vlan 2
Outgoing interface list:
  GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
Incoming vlan: Vlan 2
Outgoing interface list:
  GigabitEthernet 4/11
  GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
Incoming vlan: Vlan 2
Outgoing interface list:
  GigabitEthernet 4/11
  GigabitEthernet 4/13
  GigabitEthernet 4/20

Example (VLT) Dell# show ip mroute vlt
IP Multicast Routing Table
Flags: S - Synced
(*, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
Spanned outgoing interface list:
  Vlan 20 (S)
Vlan 30
(50.1.1.2, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
Spanned outgoing interface list:
Vlan 20 (S)

Usage Information
The following describes the `show ip mroute` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the forwarding entry in the multicast route table.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the multicast forwarding table.</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following:</td>
</tr>
<tr>
<td></td>
<td>• a directly connected member of the Group</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) or (S,G) Join message</td>
</tr>
</tbody>
</table>

Example
Dell# show ip mroute
IP Multicast Routing Table
(*, 224.10.10.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
    GigabitEthernet 3/13
(1.13.1.100, 224.10.10.1), uptime 00:04:03
Incoming interface: GigabitEthernet 3/4
Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13
(*, 224.20.20.1), uptime 00:05:12
Incoming interface: GigabitEthernet 3/12
Outgoing interface list:
    GigabitEthernet 3/4

**show ip rpf**

View reverse path forwarding.

Syntax
```
show ip rpf
```

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Usage Information**

Network administrators use static mroutes to control the reachability 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 reachability.

**NOTE:** The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

**Example**

Dell# show ip rpf
RPF information for 10.10.10.9
   RPF interface: Gi 3/4
   RPF neighbor: 165.87.31.4
   RPF route/mask: 10.10.10.9/255.255.255.255
   RPF type: unicast
Neighbor Discovery Protocol (NDP)

The neighbor discovery protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery — hosts can locate routers residing on a link
- Prefix discovery — hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD) — determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD) — allow a node to check whether a proposed address is already in use.
- Redirect — the router can inform a node about a better first-hop.

NDP uses the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Topics:

- clear ipv6 neighbors
- ipv6 neighbor
- show ipv6 neighbors
- IPv6 Router Advertisement (RA) Guard

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 [vrf vrf-name] [ipv6-address | interface]
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to clear the neighbor corresponding to that VRF.

**NOTE:** If you do not specify this option, the neighbors in the default VRF are cleared.
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.

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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

**Syntax**

```
ipv6 neighbor [vrf vrf-name] {ipv6-address} {interface interface} {hardware_address}
```

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor [vrf vrf-name] {ipv6-address} {interface interface} {hardware_address}` command.

**Parameters**

- **vrf vrf-name**
  (Optional) Enter the keyword vrf followed by the name of the VRF to install IPv6 routes in that VRF.
- **ipv6-address**
  Enter the IPv6 address of the neighbor in the x:x:x::x format.
NOTE: The :: notation specifies successive hexadecimal fields of zero.

**interface interface**  
Enter the keyword `interface` then the interface type and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a Null interface, enter the keyword `null` then the Null interface number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number.
  The range is from 1 to 16383.

**hardware_address**  

**Defaults**  
None

**Command Modes**  
CONFIGURATION

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(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.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.1 | Introduced on the S4810.

**Usage Information**  
Neighbor Discovery Protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. It defines mechanisms for solving problems, such as:

- Router discovery: Hosts can locate routers residing on a link.
- Prefix discovery: Hosts can discover address prefixes for the link.
- Parameter discovery.
- Address autoconfiguration — configuration of addresses for an interface.
- Address resolution — mapping from IP address to link-layer address.
- Next-hop determination.
- Neighbor Unreachability Detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate Address Detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.
Use the `ipv6 neighbor` command to manually configure the IPv6 address of a neighbor to be discovered by the switch.

**show ipv6 neighbors**

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the control processor (CP).

**Syntax**

```
show ipv6 neighbors [vrf vrf-name] [ipv6-address| interface interface]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` and the name of the VRF to display the neighbors corresponding to that VRF.
  
  **NOTE:** If you do not specify this option, neighbors corresponding to the default VRF are displayed.

- `ipv6-address` Enter the IPv6 address of the neighbor in the `x:x:x:x::x` format.
  
  **NOTE:** The `::` notation specifies successive hexadecimal fields of zero.

- `interface interface` Enter the keyword `interface` then the interface type and slot/port or number information:
  
  - For a `1-GigabitEthernet` interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a `10-Gigabit Ethernet` interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Management interface, enter the keyword `managementethernet` followed by the slot/port numbers.
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - For a port channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

None

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
IPv6 Router Advertisement (RA) Guard

The IPv6 RA guard provides support to perform conditional forwarding or blocking of the router advertisement messages that are received at the network device platform. This functionality analyzes and filters the RAs sent by the devices and compares the configuration information on the layer 2 device with the RA frame. Once the layer 2 device validates the content of the RA frame against the configuration, it forwards the RA to its unicast or multicast destination. On failure to validate the RA frame content, the RA frame is dropped.

The IPv6 RA guard supports two different modes:

- **Host mode** — When a policy with device role as host is applied on an interface, all the RA packets are dropped without validation. You can also configure the host mode policy with VLAN option to drop the RA packets on that specific VLAN and port.
- **Router mode** — When a policy with device role as router is applied on an interface, all the RA packets are validated based on the configuration information in the policy. Similarly, you can also apply this mode over any specific VLAN and the validation is performed only for that particular VLAN RA packets.

To configure the IPv6 RA guard, use the following Dell Networking OS commands.

### debug ipv6 nd ra-guard

Enable debugging for IPv6 RA guard snooping information.

| Syntax            | debug ipv6 nd ra-guard [interface_type slot/port | count value] |
|-------------------|-----------------------------------------------|
| Parameters        | interface_type slot/port                     |
| count value       | Enter the keyword count then the number of debug outputs. The range is from 1 to 65534. The default is infinity. |
| Defaults          | None                                           |
| Command Modes     | EXEC Privilege                                |
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**device-role**

Specify the role of the device attached to the port.

**Syntax**
```
device-role {host | router}
```

To reset the device role, use the `no device-role {host | router}` command.

**Parameters**

- **host**: Enter the keyword `host` to set the device-role as host.
- **router**: Enter the keyword `router` to set the device-role as router.

**Defaults**
None

**Command Modes**
POLICY LIST CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Related Commands**
- `ipv6 nd raguard policy policy-name` — define the RA guard policy name and enter the RA guard policy configuration mode.
- `ipv6 nd ra-guard enable` — configure the RA guard related commands.

**hop-limit**

Enable the verification of the advertised hop count limit. If this command is not configured, the verification process is bypassed.

**Syntax**
```
hop-limit {maximum | minimum limit}
```

To reset the hop count limit, use the `no hop-limit {maximum | minimum limit}` command.
**Parameters**

- **maximum limit**
  - Enter the keyword maximum then the hop limit value. The range is from 0 to 254.
- **minimum limit**
  - Enter the keyword minimum then the hop limit value. The range is from 0 to 254.

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ipv6 nd ra-guard enable` — configure the RA guard related commands.
- `ipv6 nd ra-guard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

**ipv6 nd ra-guard attach-policy**

Apply the IPv6 RA guard to a specific interface.

**Syntax**

```
ipv6 nd ra-guard attach-policy policy-name [vlan [vlan 1, vlan 2, vlan 3.....]]
```

**Parameters**

- **policy policy-name**
  - Enter the keyword policy then the policy name. The policy-name allows a maximum of 140 characters.
- **vlan [vlan 1, vlan 2, vlan 3........]**
  - Enter the keyword vlan then the VLAN range. The VLAN range is from 1 to 4094.

**Defaults**

None

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>
(ipv6 nd ra-guard policy

Define the RA guard policy name and enter the RA guard policy list configuration mode.

Syntax

```
ipv6 nd ra-guard policy policy-name
```

Parameters

- **policy policy-name**: Enter the keyword policy then the policy-name. The policy name allows a maximum of 140 characters.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>
Related Commands

- `ipv6 nd ra-guard enable` — configure the RA guard related commands.

### managed-config-flag

Set the managed address configuration flag.

**Syntax**

```plaintext
managed-config-flag {on | off}
```

To clear the flag, use the `no managed-config-flag {on | off}` command.

**Parameters**

- `on` — Enter the keyword `on` to set the managed-config-flag value as ON.
- `off` — Enter the keyword `off` to set the managed-config flag value as OFF.

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ipv6 nd ra-guard enable` — configure the RA guard related commands.
- `ipv6 nd raguard policy policy-name` — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

### match ra

Enable verifying either of the configured source IPv6 address or prefix address or the source MAC address in the inspected messages. If this command is not configured, the verification process is bypassed.

**Syntax**

```plaintext
match ra {ipv6-access-list name | ipv6-prefix-list name | mac-access-list name}
```

To reset the access list, use the `no match ra {ipv6-access-list | ipv6-prefix-list | mac-access-list}` command.

**Parameters**

- `ipv6-access-list name` — Enter the keywords `ipv6-access-list` then the access-list name. The access-list name allows a maximum of 140 characters.
- `ipv6-prefix-list name` — Enter the keywords `ipv6-prefix-list` then the prefix-list name. The prefix-list name allows a maximum of 140 characters.
- `ipv6-mac-access-list name` — Enter the keywords `ipv6-mac-access-list` then the mac-access-list name. The mac-access-list name allows a maximum of 140 characters.
mtu

Enable the verification of the configured maximum transmission unit (MTU) value in the received RA packets.

Syntax

mtu value

To reset the MTU value, use the no mtu value command.

Parameters

value

Enter the maximum transmission unit value in bytes. The range is from 1,280 to 11,982 bytes.

Defaults

0

Command Modes

POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.9(0.0) Introduced on the Z9500.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000–ON.
9.7(0.0) Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.
**other-config-flag**

Enable the verification of the advertised other configuration parameter. If this command is not configured, the verification process is bypassed.

**Syntax**

```
other-config-flag {on | off}
```

To reset the other configuration parameter, use the `no other-config-flag {on | off}` command.

**Parameters**

- **on**: Enter the keyword `on` to set the other-config-flag value as ON.
- **off**: Enter the keyword `off` to set the other-config-flag value as OFF.

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ipv6 nd ra-guard enable` — configure the RA guard related commands.
- `ipv6 nd raguard policy policy-name` — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

**reachable-time**

Enable the verification of the configured reachability time in the received RA packets.

**Syntax**

```
reachable-time value
```

To reset the advertised reachability time, use the `no reachable-time value` command.

**Parameters**

- **value**: Enter the advertised reachability time in milliseconds. The range is from 0 to 3,600,000 milliseconds.

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
retrans-time

Enable the verification of the configured retransmission timer value in the received RA packets.

Syntax
retrans—timer value

To reset the advertised retransmission interval, use the no retrans—timervalue command.

Parameters
value
Enter the advertised retransmission time interval in milliseconds. The range is from 100 to 4,294,967,295 milliseconds.

Defaults
None

Command Modes
POLICY LIST CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.9(0.0) Introduced on the Z9500.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands
- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

router-lifetime

Set the router lifetime.

Syntax
router-lifetime value

Related Commands
- ipv6 nd ra-guard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.
- ipv6 nd ra-guard enable — configure the RA guard related commands.
**Parameters**

| value | Enter the router lifetime in seconds. The range is from 0 to 9,000 seconds. |

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ipv6 nd ra-guard enable` — configure the RA guard related commands.
- `ipv6 nd raguard policy policy-name` — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

---

**router-preference maximum**

Enable the verification of the advertised default router preference (DRP) value. The preference value is lower than or equal to the specified limit. If this command is not configured, the verification process is bypassed.

**Syntax**

```
router-preference maximum {high | low | medium}
```

To reset the default router preference value, use the `no router-preference maximum {high | low | medium}` command.

**Parameters**

| high | Enter the keyword `high` to set the DRP value as high. |
| low | Enter the keyword `low` to set the DRP value as low. |
| medium | Enter the keyword `medium` to set the DRP value as medium. |

**Defaults**

None

**Command Modes**

POLICY LIST CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>
show config

Display the RA guard policy mode configurations.

**Syntax**
show config

**Command Modes**
POLICY LIST CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

**Example**
Dell(conf)# ipv6 nd ra-guard policy test
Dell(conf-ra_guard_policy_list)#show config
!
ipv6 nd ra-guard policy test
device-role router
hop-limit maximum 251
mtu 1350
other-config-flag on
reachable-time 540
retrans-timer 101
router-preference maximum medium
trusted-port
Dell(conf-ra_guard_policy_list)#

**Related Commands**
- `ipv6 nd ra-guard enable` — configure the RA guard related commands.
- `ipv6 nd ra-guard policy` — define the RA guard policy name and enter the RA guard policy list configuration mode.
- `device-role` — specify the role of the device attached to the port.
- `hop-limit` — enable the verification of the advertised hop count limit.
- `mtu` — set the maximum transmission unit (MTU) value.
- `other-config-flag` — enable the verification of the advertised other configuration parameter.
- `reachable-time` — set the advertised reachability time.
- `retrans-timer` — set the advertised retransmission time.
- `router-preference maximum` — enable the verification of the advertised default router preference (DRP) value.
- `trusted-port` — apply the policy to trusted ports.
show ipv6 nd ra-guard policy

Display the configurations applied on all the RA guard policies or a specific RA guard policy.

Syntax

show ipv6 nd ra-guard policy policy-name

Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy policy-name</td>
<td>Enter the keyword <code>policy</code> then the policy name. The policy name allows a maximum of 140 characters.</td>
</tr>
</tbody>
</table>

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, Introduced on the S6000–ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

Example

Dell# show ipv6 nd ra-guard policy test
ipv6 nd ra-guard policy test
  device-role router
  hop-limit maximum 1
  match ra ipv6-access-list access
  other-config-flag on
  router-preference maximum medium
  trusted-port
  Interfaces :
  Gi 1/1
Dell#

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd ra-guard policy — define the RA guard policy name and enter the RA guard policy list configuration mode.
- device-role — specify the role of the device attached to the port.
- hop-limit — enable the verification of the advertised hop count limit.
- mtu — set the maximum transmission unit (MTU) value.
- other-config-flag — enable the verification of the advertised other configuration parameter.
- reachable-time — set the advertised reachability time.
- retrans-timer — set the advertised retransmission time.
- router-preference maximum — enable the verification of the advertised default router preference (DRP) value.
- trusted-port — apply the policy to trusted ports.
- ipv6 nd raguard attach-policy — apply the IPv6 RA guard to a specific interface.
trusted-port

Allow bypassing the configured RA guard validation and forwards the RA packets received on the interface, which has the trusted port policy attached.

Syntax

trusted-port

To reset the policy applied to the trusted port, use the no trusted-port command.

Defaults

None

Command Modes

POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.</td>
</tr>
</tbody>
</table>

Usage Information

Use this command to disable all the RA guard policies.

Related Commands

- **ipv6 nd ra-guard enable** — configure the RA guard related commands.
- **ipv6 nd raguard policy policy-name** — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.
Object Tracking supports IPv4 and IPv6, and is available on the Dell Networking platforms. Object tracking allows you to define objects of interest, monitor their state, and report to a client when a change in an object’s state occurs. The following tracked objects are supported:

- Link status of Layer 2 interfaces
- Routing status of Layer 3 interfaces (IPv4 and IPv6)
- Reachability of IPv4 and IPv6 routes
- Metric thresholds of IPv4 and IPv6 routes

You can configure client applications, such as virtual router redundancy protocol (VRRP), to receive a notification when the state of a tracked object changes.

Topics:
- IPv4 Object Tracking Commands
- IPv6 Object Tracking Commands

### IPv4 Object Tracking Commands

The following section describes the IPv4 VRRP commands.

**debug track**

Enables debugging for tracked objects.

**Syntax**

```
debug track [all | notifications | object-id]
```

**Parameters**

- `all` Enables debugging on the state and notifications of all tracked objects.
- `notifications` Enables debugging on the notifications of all tracked objects.
- `object-id` Enables debugging on the state and notifications of the specified tracked object. The range is 1 to 500.

**Defaults**

Enable debugging on the state and notifications of all tracked objects (`debug track all`).

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
8.3(12.0) | Introduced on the S4810.
8.4(1.0) | Introduced.

Example

Dell# debug track all
04:35:04: %RPM0-P:RP2 %OTM-5-STATE: track 6 - Interface GigabitEthernet 1/2 line-protocol DOWN
04:35:04: %RPM0-P:RP2 %OTM-5-NOTIF: VRRP notification: resource ID 6 DOWN

**delay**

Configure the time delay used before communicating a change in the status of a tracked object to clients.

**Syntax**

delay {up seconds} [down seconds]

To return to the default setting, use the no delay command.

**Parameters**

- **seconds**
  Enter the number of seconds the object tracker waits before sending a notification about the change in the UP and/or DOWN state of a tracked object to clients. The range is 0 to 180. The default is 0 seconds.

**Defaults**

0 seconds

**Command Modes**

OBJECT TRACKING (conf_track_object-id)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
8.3(12.0) | Introduced on the S4810.
8.4(1.0) | Introduced.

**Usage Information**

You can configure an UP and/or DOWN timer for each tracked object to set the time delay before a change in the state of a tracked object is communicated to clients. The configured time delay starts when the state changes from UP to DOWN or vice-versa.
If the state of an object changes back to its former UP/DOWN state before the timer expires, the timer is cancelled and the client is not notified. For example, if the DOWN timer is running when an interface goes down and comes back up, the DOWN timer is cancelled and the client is not notified of the event.

If the timer expires and an object’s state has changed, a notification is sent to the client. If no delay is configured, a notification is sent immediately after a change in the state of a tracked object is detected. The time delay in communicating a state change is specified in seconds.

**Related Commands**

- track interface ip routing – configure object tracking on the routing status of an IPv4 Layer 3 interface.
- track interface line-protocol – configure object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configure object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configure object tracking on the reachability of an IPv4 route.

**description**

Enter a description of a tracked object.

**Syntax**

description {text}

To remove the description, use the no description {text} command.

**Parameters**

text Enter a description to identify a tracked object (80 characters maximum).

**Defaults**

None

**Command Modes**

OBJECT TRACKING (conf_track_object-id)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- track interface ip routing – configure object tracking on the routing status of an IPv4 Layer 3 interface.
- track interface line-protocol – configure object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configure object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configure object tracking on the reachability of a specific IP address. Policy-based Routing uses the track command to track the next-hop ip address.
show running-config track

Display the current configuration of tracked objects.

Syntax

```
show running-config track [object-id]
```

Parameters

```
object-id
```

(OPTIONAL) Display information on the specified tracked object. The range is 1 to 500.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show running-config track

track 1 ip route 23.0.0.0/8 reachability
track 2 ipv6 route 2040::/64 metric threshold
delay down 3
delay up 5
threshold metric up 200
track 3 ipv6 route 2050::/64 reachability
track 4 interface GigabitEthernet 1/2 ip routing
track 5 ip route 192.168.0.0/24 reachability vrf red
track resolution ip route isis 20
track resolution ip route ospf 10
```

Example (Object-id)

```
Dell# show running-config track 300

track 300 ip route 10.0.0.0/8 metric threshold
delay down 3
delay up 5
threshold metric up 100
```

Related Commands

- `show track` – display information about tracked objects, including configuration, current state, and clients which track the object.
- `track interface ip routing` – configure object tracking on the routing status of an IPv4 Layer 3 interface.
- `track interface line-protocol` – configure object tracking on the line-protocol state of a Layer 2 interface.
- `track ip route metric threshold` – configure object tracking on the threshold of an IPv4 route metric.
- `track ip route reachability` – configure object tracking on the reachability of an IPv4 route.
show track

Display information about tracked objects, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

**Syntax**

```
show track [object-id [brief] | interface [brief] [vrf vrf-name] | ip route [brief] [vrf vrf-name] | resolution | vrf vrf-name [brief] | brief]
```

**Parameters**

- `object-id` (OPTIONAL) Display information on the specified tracked object. The range is 1 to 500.
- `interface` (OPTIONAL) Display information on all tracked interfaces (Layer 2 and IPv4 Layer 3).
- `ip route` (OPTIONAL) Display information on all tracked IPv4 routes.
- `resolution` (OPTIONAL) Display information on the configured resolution values used to scale protocol-specific route metrics. The range is 0 to 255.
- `brief` (OPTIONAL) Display a single line summary of the tracking information for a specified object, object type, or all tracked objects.
- `vrf vrf-name` (OPTIONAL) E-Series only: Display information on only the tracked objects that are members of the specified VRF instance. The maximum is 32 characters. If you do not enter a VRF name, information on the tracked objects from all VRFs displays.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show track` command shown in the Example below.

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track object-id</td>
<td>Displays the number of the tracked object.</td>
</tr>
<tr>
<td>Interface type slot/</td>
<td>Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is</td>
</tr>
<tr>
<td>port, IP route ip-</td>
<td>being tracked.</td>
</tr>
<tr>
<td>address, IPv6 route</td>
<td></td>
</tr>
<tr>
<td>ipv6-address</td>
<td></td>
</tr>
<tr>
<td>object is Up/Down</td>
<td>Up/Down state of tracked object; for example, IPv4 interface, reachability or metric</td>
</tr>
<tr>
<td>number changes,</td>
<td>threshold of an IP route.</td>
</tr>
<tr>
<td>last change time</td>
<td>Number of times that the state of the tracked object has changed and the time since the</td>
</tr>
<tr>
<td></td>
<td>last change in <code>hours:minutes:seconds</code>.</td>
</tr>
<tr>
<td>First hop interface</td>
<td>Displays the type and slot/port number of the first-hop interface of the tracked route.</td>
</tr>
</tbody>
</table>
**Output**

**Description**

**Tracked by**

Client that is tracking an object's state; for example, VRRP.

**Example**

Dell# show track

Track 1
IP route 23.0.0.0/8 reachability
Reachability is Down (route not in route table)
2 changes, last change 00:16:08
Tracked by:

Track 2
IPv6 route 2040::/64 metric threshold
Metric threshold is Up (STATIC/0/0)
5 changes, last change 00:02:16
Metric threshold down 255 up 254
First-hop interface is GigabitEthernet 1/2
Tracked by:
VRRP GigabitEthernet 2/3 IPv6 VRID 1

Track 3
IPv6 route 2050::/64 reachability
Reachability is Up (STATIC)
5 changes, last change 00:02:16
First-hop interface is GigabitEthernet 1/2
Tracked by:
VRRP GigabitEthernet 2/3 IPv6 VRID 1

**Usage Information**

The following describes the show track brief command shown in the Example below.

**Output**

**Description**

**ResID**
Number of the tracked object.

**Resource**
Type of tracked object.

**Parameter**
Detailed description of the tracked object.

**State**
Up or Down state of the tracked object.

**Last Change**
Time since the last change in the state of the tracked object.

**Example (Brief)**

Dell> show track brief
ResID Resource Parameter State LastChange
1 IP route reachability 10.16.0.0/16 Up 00:01:08
2 Interface line-protocol Ethernet0/2 Down 00:05:00
3 Interface ip routing VLAN100 Up 01:10:05

**Related Commands**

- `show running-config track` – display configuration information about tracked objects.
- `track interface ip routing` – configure object tracking on the routing status of an IPv4 Layer 3 interface.
- `track interface line-protocol` – configure object tracking on the line-protocol state of a Layer 2 interface.
- `track ip route metric threshold` – configure object tracking on the threshold of an IPv4 route metric.
- `track ip route reachability` – configure object tracking on the reachability of an IPv4 route.

**threshold metric**

Configure the metric threshold used to determine the UP and/or DOWN state of a tracked IPv4 or IPv6 route.

**Syntax**

```
threshold metric {up number | down number}
```

[[985]]
To return to the default setting, use the `no threshold metric {up number | down number}` command.

**Parameters**

- **up number**
  Enter a number for the UP threshold to be applied to the scaled metric of an IPv4 or IPv6 route. The default UP threshold is 254. The routing state is UP if the scaled route metric is less than or equal to the UP threshold.

- **down number**
  Enter a number for the DOWN threshold to be applied to the scaled metric of an IPv4 or IPv6 route. The default DOWN threshold is 255. The routing state is DOWN if the scaled route metric is greater than or equal to the DOWN threshold.

**Defaults**

None

**Command Modes**

OBJECT TRACKING (conf_track_object-id)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to configure the UP and/or DOWN threshold for the scaled metric of a tracked IPv4 or IPv6 route.

Determine the UP/DOWN state of a tracked route by the threshold for the current value of the route metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value.

The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

Configure the UP and DOWN thresholds for each tracked route with the `threshold metric` command. The default UP threshold is 254; the default DOWN threshold is 255. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

The tracking process uses a protocol-specific resolution value to convert the actual metric in the routing table to a scaled metric in the range 0 to 255. You can configure the resolution value used to scale route metrics for supported protocols with the `track resolution ip route` and `track resolution ipv6 route` commands.

**Related Commands**

- `track ip route metric threshold` — configure object tracking on the threshold of an IPv4 route metric.
- `track resolution ip route` — configure the protocol-specific resolution value used to scale an IPv4 route metric.
**track interface ip routing**

Configure object tracking on the routing status of an IPv4 Layer 3 interface.

**Syntax**

```plaintext
track object-id interface interface ip routing
```

To return to the default setting, use the `no track object-id` command.

**Parameters**

- **object-id**
  - Enter the ID number of the tracked object. The range is 1 to 500.

- **interface**
  - Enter one of the following values:
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
    - For a port channel interface, enter the keywords `port-channel` then a number.
    - For a tunnel interface, enter the keyword `tunnel`.
    - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON. Added support for <code>tunnel</code> interface.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to create an object that tracks the routing state of an IPv4 Layer 2 interface:

- The status of the IPv4 interface is UP only if the Layer 2 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv4 interface goes DOWN when its Layer 2 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.

**Related Commands**

- `show track` — display information about tracked objects, including configuration, current state, and clients which track the object.
- `track interface line-protocol` — configure object tracking on the line-protocol state of a Layer 2 interface.
track interface line-protocol

Configure object tracking on the line-protocol state of a Layer 2 interface.

Syntax

```
track object-id interface interface line-protocol
```

To return to the default setting, use the no track object-id command.

Parameters

- **object-id**
  - Enter the ID number of the tracked object. The range is 1 to 500.

- **interface**
  - Enter one of the following values:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a 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 tunnel interface, enter the keyword tunnel.
    - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

Use this command to create an object that tracks the line-protocol state of a Layer 2 interface by monitoring its operational status (UP or DOWN).

When the link-level status goes down, the tracked object status is considered to be DOWN; if the link-level status is up, the tracked object status is considered to be UP.

Related Commands

- `show track` — display information about tracked objects, including configuration, current state, and clients which track the object.
- `track interface ip routing` — configure object tracking on the routing status of an IPv4 Layer 3 interface.
track ip host reachability

Configure object tracking on the reachability of an IPv4 host.

Syntax

```
track object-id ip host host-ip-address/prefix-len reachability [vrf vrf-name]
```

To return to the default setting, use the `no track object-id` command.

Parameters

- `object-id` Enter the ID number of the tracked object. The range is 1 to 500.
- `ip-address/prefix-len` Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.
- `vrf vrf-name` (Optional) You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4820T, S4810, S6000, S5000, Z9000, Z9500, IOA, and MXL.</td>
</tr>
</tbody>
</table>

track ip route metric threshold

Configure object tracking on the threshold of an IPv4 route metric.

Syntax

```
track object-id ip route ip-address/prefix-len metric threshold [vrf vrf-name]
```

To return to the default setting, use the `no track object-id` command.

Parameters

- `object-id` Enter the ID number of the tracked object. The range is 1 to 500.
- `ip-address/prefix-len` Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.
- `vrf vrf-name` (Optional) E-Series only: You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
Track IP Route Reachability

Configure object tracking on the reachability of an IPv4 route.

Syntax

```
track object-id ip route ip-address/prefix-len reachability [vrf vrf-name]
```

To return to the default setting, use the `no track object-id` command.

Parameters

- `object-id` Enter the ID number of the tracked object. The range is 1 to 500.
- `ip-address/prefix-len` Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.
vrf vrf-name

(Optional) E-Series only: You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

Defaults
None

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
8.3.12.0 Introduced on the S4810.
8.4.1.0 Introduced.

Usage Information
Use this command to create an object that tracks the reachability of an IPv4 route. In order for a route’s reachability to be tracked, the route must appear as an entry in the routing table.

A tracked IPv4 route is considered to match an entry in the routing table only if the exact IPv4 address and prefix length match a table entry. For example, when configured as a tracked route, 10.0.0.0/24 does not match the routing table entry 10.0.0.0/8. If no route-table entry has the exact IPv4 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure IPv4 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the ARP cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route’s next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry to if the next-hop address appears before considering the route DOWN.

Related Commands
- `show track` — display information about tracked objects, including configuration, current state, and clients which track the object.
- `track ip route metric threshold` — configure object tracking on the threshold of an IPv4 route metric.

track resolution ip route

Configure the protocol-specific resolution value used to scale an IPv4 route metric.

Syntax
```
track resolution ip route {isis resolution-value | ospf resolution-value}
```
To return to the default setting, use the `no track object-id` command.

Parameters
- `object-id` Enter the ID number of the tracked object. The range is 1 to 500.
- `isis resolution-value` Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
 ospf resolution-value

Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv4 route in the routing table to a scaled metric in the range 0 to 255.

The UP/DOWN state of a tracked IPv4 route is determined by a user-configurable threshold (the threshold metric command) for the route’s metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route’s cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1.
- The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes.
- The resolution value used to map RIP routes is not configurable. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.

Related Commands

- threshold metric — configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- track ip route metric threshold — configure object tracking on the threshold of an IPv4 route metric.

IPv6 Object Tracking Commands

The following section describes the IPv6 object tracking commands.

The following object tracking commands apply to IPv4 and IPv6:

- debug track
- delay
- description
- show running-config track
- threshold metric
**show track ipv6 route**

Display information about all tracked IPv6 routes, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

**Syntax**

```
show track ipv6 route [brief]
```

**Parameters**

- **brief**  
  (OPTIONAL) Display a single line summary of information for tracked IPv6 routes.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show track ipv6 route` command shown in the Example below.

**Output**

- **Track object-id**
  Displays the number of the tracked object.

- **Interface type slot/port, IP route ip-address, IPv6 route ipv6-address**
  Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.

- **object is Up/Down**
  Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.

- **number changes, last change time**
  Number of times that the state of the tracked object has changed and the time since the last change in `hours:minutes:seconds`.

- **First hop interface**
  Displays the type and slot/port number of the first-hop interface of the tracked route.

- **Tracked by**
  Client that is tracking an object’s state; for example, VRRP.

**Example**

```
Dell# show track ipv6 route

Track 2
IPv6 route 2040::/64 metric threshold
Metric threshold is Up (STATIC/0/0)
  5 changes, last change 00:02:30
Metric threshold down 255 up 254
First-hop interface is GigabitEthernet 1/2
Tracked by:
  VRRP GigabitEthernet 2/4 IPv6 VRID 1
```
Track 3
IPv6 route 2050::/64 reachability
Reachability is Up (STATIC)
  5 changes, last change 00:02:30
First-hop interface is GigabitEthernet 1/2
  Tracked by:
    VRRP GigabitEthernet 2/4 IPv6 VRID 1

Usage Command
The following describes the show track ipv6 route brief command shown in the Example below.

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResId</td>
<td>Number of the tracked object.</td>
</tr>
<tr>
<td>Resource</td>
<td>Type of tracked object.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Detailed description of the tracked object.</td>
</tr>
<tr>
<td>State</td>
<td>Up or Down state of the tracked object.</td>
</tr>
<tr>
<td>Last Change</td>
<td>Time since the last change in the state of the tracked object.</td>
</tr>
</tbody>
</table>

Example (Brief)
Dell# show track ipv6 route brief

<table>
<thead>
<tr>
<th>ResId</th>
<th>Resource</th>
<th>Parameter</th>
<th>State</th>
<th>LastChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>IPv6 route metric threshold 2040::/64</td>
<td>Up</td>
<td>00:02:36</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>IPv6 route reachability 2050::/64</td>
<td>Up 00:02:36</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Commands
- show running-config track – display configuration information about tracked objects.
- show track – display information about tracked objects, including configuration, current state, and clients which track the object.
- track interface ipv6 routing – configure object tracking on the routing status of an IPv6 Layer 3 interface.
- track ipv6 route metric threshold – configure object tracking on the threshold of an IPv6 route metric.
- track ipv6 route reachability – configure object tracking on the reachability of an IPv6 route.

track interface ipv6 routing

Configure object tracking on the routing status of an IPv6 Layer 3 interface.

Syntax
track object-id interface interface ipv6 routing

To return to the default setting, use the no track object-id command.

Parameters
- **object-id**
  Enter the ID number of the tracked object. The range is 1 to 500.
- **interface**
  Enter one of the following values:
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For a port channel interface, enter the keywords port-channel then a number.
  - For a tunnel interface, enter the keyword tunnel.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
None
track ipv6 route metric threshold

Configure object tracking on the threshold of an IPv4 route metric.

Syntax

```
track object-id ipv6 route ipv6-address/prefix-len metric threshold
```

To return to the default setting, use the `no track object-id` command.

Parameters

- `object-id` : Enter the ID number of the tracked object. The range is 1 to 500.
- `ipv6-address/prefix-len` : Enter an IPv6 address in X:X::X format. The valid IPv6 prefix lengths are from /0 to /128.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

Use this command to create an object that tracks the routing state of an IPv6 Layer 3 interface:

- The status of the IPv6 interface is UP only if the Layer 2 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv6 interface goes DOWN when its Layer 2 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.

Related Commands

- `show track ipv6 route` — display information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- `track interface ip routing` — configure object tracking on the routing status of an IPv4 Layer 3 interface.
track ipv6 route reachability

Configure object tracking on the reachability of an IPv6 route.

Syntax

track object-id ipv6 route ip-address/prefix-len reachability

To return to the default setting, use the no track object-id command.

Parameters

- **object-id**
  - Enter the ID number of the tracked object. The range is 1 to 500.
- **ipv6-address/prefix-len**
  - Enter an IPv6 address in X:X:X:X::X format. The valid IPv6 prefix lengths are from /0 to /128.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version     Description
9.8(1.0)    Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)    Introduced on the S6000-ON.
8.3.12.0    Introduced on the S4810.
8.4.1.0     Introduced.

Usage Information
Use this command to create an object that tracks the reachability of an IPv6 route. In order for a route’s reachability to be tracked, the route must appear as an entry in the routing table.

A tracked route is considered to match an entry in the routing table only if the exact IPv6 address and prefix length match a table entry. For example, when configured as a tracked route, 3333:100:200:300:400::/80 does not match routing table entry 3333:100:200:300::/64. If no route-table entry has the exact IPv6 address and prefix length, the tracked route is considered to be DOWN.

When you configure IPv6 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the ARP cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route's next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry to if the next-hop address appears before considering the route DOWN.

Related Commands
- `show track ipv6 route` – display information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- `track ipv6 route reachability` – configure object tracking on the reachability of an IPv4 route.

track resolution ipv6 route

Configure the protocol-specific resolution value used to scale an IPv6 route metric.

Syntax
```
track resolution ipv6 route {isis resolution-value | ospf resolution-value}
```

To return to the default setting, use the `no track object-id` command.

Parameters
- **object-id**
  - Enter the ID number of the tracked object. Use the range to 1 to 500.
- **isis resolution-value**
  - Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
- **ospf resolution-value**
  - Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.

Defaults
- None

Command Modes
- CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv6 route in the routing table to a scaled metric in the range 0 to 255.

The UP/DOWN state of a tracked IPv6 route is determined by the user-configurable threshold (the `threshold metric` command) for a route's metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route's cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1.
- The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes.
- The resolution value used to map RIP routes is not configurable. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.

**Related Commands**

- `threshold metric` — configure the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- `track ipv6 route metric threshold` — configure object tracking on the threshold of an IPv6 route metric.
Open Shortest Path First (OSPFv2 and OSPFv3)

Open Shortest Path First version 2 for IPv4 is supported on platform.
OSPF is an interior gateway protocol (IGP), which means that it distributes routing information between routers in a single autonomous system (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) are the same for OSPFv2 and OSPFv3. OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

This section 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.

NOTE: Dell Networking OS version 7.8.1.0 introduces Multi-Process OSPF on IPv4 (OSPFv2) only. It is not supported on OSPFv3 (IPv6).
The CLI requires that you include the Process ID when entering ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

Topics:
- OSPFv2 Commands
- OSPFv3 Commands

OSPFv2 Commands

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328.

area default-cost

Set the metric for the summary default route the area border router (ABR) generates into the stub area. Use this command on the border routers at the edge of a stub area.

S3048–ON

Syntax

area area-id default-cost cost

To return default values, use the no area area-id default-cost command.

Parameters

area-id

Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.

cost

Specifies the stub area's advertised external route metric. The range is from zero (0) to 65535.

Defaults

cost = 1; no areas are configured.
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

In the Dell Networking operating software (OS), cost is defined as reference bandwidth/bandwidth.

Related Commands

- area stub — create a stub area.

**area nssa**

Specify an area as a not so stubby area (NSSA).

**S3048-ON**

**Syntax**

area area-id nssa [default-information-originate] [no-redistribution] [no-summary]

To delete an NSSA, use the no area area-id nssa command.

**Parameters**

- **area-id**
  Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
- **no-redistribution** (OPTIONAL) Specify that the redistribute command does not distribute routes into the NSSA. Only use this command in an NSSA area border router (ABR).
- **default-information-originate** (OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
- **no-summary** (OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

**Defaults**

Not configured.
Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

area range

Summarize routes matching an address/mask at an area border router (ABR).

S3048-ON

Syntax

area area-id range ip-address mask [not-advertise]

To disable route summarization, use the no area area-id range ip-address mask command.

Parameters

- **area-id**: Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
- **ip-address**: Specify an IP address in dotted decimal format.
- **mask**: Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
- **not-advertise** (OPTIONAL) Enter the keywords not-advertise to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults

Not configured.

Command Modes

ROUTER OSPF
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands

- area stub — create a stub area.
- router ospf — enter ROUTER OSPF mode to configure an OSPF instance.

area stub

Configure a stub area, which is an area not connected to other areas.

S3048–ON

Syntax

area area-id stub [no-summary]

To delete a stub area, use the no area area-id stub command.

Parameters

- area-id Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from zero (0) to 65535.
- no-summary (OPTIONAL) Enter the keywords no-summary to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults

Disabled.

Command Modes

ROUTER OSPF
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To configure all routers and access servers within a stub, use this command.

Related Commands

- **router ospf** — enter ROUTER OSPF mode to configure an OSPF instance.

**auto-cost**

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

**S3048-ON**

Syntax

auto-cost [reference-bandwidth ref-bw]

To return to the default bandwidth or to assign cost based on the interface type, use the no auto-cost [reference-bandwidth] command.

Parameters

- **ref-bw**

  (OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is 100 megabits per second.

Defaults

100 megabits per second.

Command Modes

- ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
clear ip ospf

Clear all OSPF routing tables.

**S3048-ON**

**Syntax**
```
clear ip ospf process-id [vrf vrf-name] [process]
```

**Parameters**
- **process-id**: Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
- **vrf vrf-name**: Enter the keyword `vrf` and then the name of the VRF to clear all OSPF routing tables corresponding to that VRF.
- **process**: (OPTIONAL) Enter the keyword `process` to reset the OSPF process.

**Command Modes**
- EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.8(0.0) | Introduced on the S5100.
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.
clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

S3048-ON

Syntax

```
clear ip ospf [process-id] [vrf vrf-name] statistics [interface name {neighbor router-id}]
```

Parameters

- **process-id**
  - Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.

- **vrf vrf-name**
  - Enter the keyword vrf followed by the name of the VRF to clear all OSPF routing tables corresponding to that VRF.

- **statistics**
  - Enter the keyword statistics to clear the packet statistics in interfaces and neighbors.

- **interface name**
  - (OPTIONAL) Enter the keyword interface then one of the following interface keywords and slot/port or number information:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
    - For a VLAN, enter the keyword vlan then a number from 1 to 4094.
    - For Port Channel groups, enter the keywords port-channel then a number.

- **neighbor router-id**
  - (OPTIONAL) Enter the keyword neighbor then the neighbor’s router-id in dotted decimal format (A.B.C.D.).

Defaults

None

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

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.

---

Open Shortest Path First (OSPFv2 and OSPFv3) | 1005
**debug ip ospf**

Display debug information on OSPF. Entering the debug ip ospf commands enables OSPF debugging for the first OSPF process.

**S3048–ON**

`debug ip ospf [process-id] [vrf vrf-name] [bfd | event | packet | spf | database-timer rate-limit]`

To cancel the debug command, use the `no debug ip ospf` command.

**Parameters**

- `process-id` Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
- `vrf vrf-name` Enter the keyword vrf to view debugging information on OSPF corresponding to that VRF.
- `bfd` (OPTIONAL) Enter the keyword bfd to debug only OSPF BFD information.
- `event` (OPTIONAL) Enter the keyword event to debug only OSPF event information.
- `packet` (OPTIONAL) Enter the keyword packet to debug only OSPF packet information.
- `spf` (OPTIONAL) Enter the keyword spf to display the Shortest Path First information.
- `database-timer rate-limit` (OPTIONAL) Enter the keywords database-timer rate-limit to display the LSA throttling timer information. This applies to the S4810 platform only.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

---

### Table: Version and Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.02.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Added the database-timer rate-limit option for the S4810.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `debug ip ospf` command shown in the Example below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:14</td>
<td>Displays the time stamp.</td>
</tr>
<tr>
<td>OSPF</td>
<td>Displays the OSPF process ID: instance ID.</td>
</tr>
<tr>
<td>v:</td>
<td>Displays the OSPF version. Dell Networking OS supports version 2 only.</td>
</tr>
<tr>
<td>t:</td>
<td>Displays the type of packet sent:</td>
</tr>
<tr>
<td></td>
<td>• 1 - Hello packet</td>
</tr>
<tr>
<td></td>
<td>• 2 - database description</td>
</tr>
<tr>
<td></td>
<td>• 3 - link state request</td>
</tr>
<tr>
<td></td>
<td>• 4 - link state update</td>
</tr>
<tr>
<td></td>
<td>• 5 - link state acknowledgement</td>
</tr>
<tr>
<td>l:</td>
<td>Displays the packet length.</td>
</tr>
<tr>
<td>rid:</td>
<td>Displays the OSPF router ID.</td>
</tr>
<tr>
<td>aid:</td>
<td>Displays the Autonomous System ID.</td>
</tr>
<tr>
<td>chk:</td>
<td>Displays the OSPF checksum.</td>
</tr>
<tr>
<td>aut:</td>
<td>States if OSPF authentication is configured. One of the following is listed:</td>
</tr>
<tr>
<td></td>
<td>• 0 - no authentication configured</td>
</tr>
<tr>
<td></td>
<td>• 1 - simple authentication configured using the <code>ip ospf authentication-key</code> command</td>
</tr>
<tr>
<td></td>
<td>• 2 - MD5 authentication configured using the <code>ip ospf message-digest-key</code> command</td>
</tr>
<tr>
<td>auk:</td>
<td>If the <code>ip ospf authentication-key</code> command is configured, this field displays the key used.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
keyid: | If the `ip ospf message-digest-key` command is configured, this field displays the MD5 key.
to: | Displays the interface to which the packet is intended.
dst: | Displays the destination IP address.
netmask: | Displays the destination IP address mask.
pr: | Displays the OSPF priority.
N, MC, E, T | Displays information available in the Options field of the HELLO packet:
  - N + (N-bit is set)
  - N - (N-bit is not set)
  - MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets)
  - MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets)
  - E + (router is able to accept AS External LSAs)
  - E - (router cannot accept AS External LSAs)
  - T + (router can support TOS)
  - T - (router cannot support TOS)
hi: | Displays the amount of time configured for the HELLO interval.
di: | Displays the amount of time configured for the DEAD interval.
dr: | Displays the IP address of the designated router.
bdr: | Displays the IP address of the Border Area Router.

Example

```
Dell# debug ip ospf 1 packet
OSPF process 90, packet debugging is on
Dell#
08:14:24 : OSPF(100:00):
  Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
    aid:0.0.0.0.1 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 Dell Networking Operating System (OS).

**Syntax**

```
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

To return to the default values, use the `no default-information originate` command.

**Parameters**

- **always**  
  (OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.

- **metric metric-value**  
  (OPTIONAL) Enter the keyword `metric` then a number to configure a metric value for the route. The range is from 1 to 16777214.

- **metric-type type-value**  
  (OPTIONAL) Enter the keywords `metric-type` then an OSPF link state type of 1 or 2 for default routes. The values are:
route-map map-name

(OPTIONAL) Enter the keywords route-map then the name of an established route map.

Defaults

Disabled.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Added support for the Multi-Process OSPF.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.

Related Commands

• redistribute — redistributes routes from other routing protocols into OSPF.

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the redistribute command.

S3048-ON

default-metric number

To return to the default values, use the no default-metric [number] command.

Parameters

number Enter a number as the metric. The range is from 1 to 16777214.

Defaults Disabled.

Command Modes ROUTER OSPF
command history

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

description

Add a description about the selected OSPF configuration.

S3048–ON

Syntax
description description
To remove the OSPF description, use the no description command.

Parameters

- **description**
  - Enter a text string description to identify the OSPF configuration (80 characters maximum).

Defaults

None

Command Modes

- ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
9.2(1.0) |Introduced on the Z9500.
9.0.2.0 |Introduced on the S6000.
8.3.19.0 |Introduced on the S4820T.
8.3.11.1 |Introduced on the Z9000.
8.3.7.0 |Introduced on the S4810.
7.8.1.0 |Introduced on the S-Series.
7.5.1.0 |Introduced on the C-Series.
pre- 6.1.1.1 |Introduced on the E-Series.

Related Commands

- show ip ospf asbr — display the VLAN configuration.

**distance**

Define an administrative distance for particular routes to a specific IP address.

### S3048-ON

**Syntax**

```plaintext
distance weight [ip-address mask access-list-name]
```

To delete the settings, use the `no distance weight [ip-address mask access-list-name]` command.

**Parameters**

- `weight` Specify an administrative distance. The range is from 1 to 255. The default is 110.
- `ip-address` (OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, include the mask for that router address.
- `mask` (OPTIONAL) Enter a mask in dotted decimal format or /n format.
- `access-list-name` (OPTIONAL) Enter the name of an IP standard access list, up to 140 characters.

**Defaults**

110

**Command Modes**

ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.8(1.0) |Introduced on the Z9100-ON.
9.8(0.0P5) |Introduced on the S4048-ON.
9.8(0.0P2) |Introduced on the S3048-ON.
9.7(0.0) |Introduced on the S6000-ON.
9.2(1.0) |Introduced on the Z9500.
distance ospf

Configure an OSPF distance metric for different types of routes.

S3048-ON

distance ospf [external \textit{dist}3] [inter-area \textit{dist}2] [intra-area \textit{dist}1]

To delete these settings, use the \texttt{no distance ospf} command.

Parameters

- \textit{external} \textit{dist}3 (OPTIONAL) Enter the keyword \textit{external} then a number to specify a distance for external type 5 and 7 routes. The range is from 1 to 255. The default is 110.
- \textit{inter-area} \textit{dist}2 (OPTIONAL) Enter the keywords \textit{inter-area} then a number to specify a distance metric for routes between areas. The range is from 1 to 255. The default is 110.
- \textit{intra-area} \textit{dist}1 (OPTIONAL) Enter the keywords \textit{intra-area} then a number to specify a distance metric for all routes within an area. The range is from 1 to 255. The default is 110.

Defaults

- \textit{external} \textit{dist}3 = 110
- \textit{inter-area} \textit{dist}2 = 110
- \textit{intra-area} \textit{dist}1 = 110

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
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.

**S3048-ON**

**Syntax**

```
distribute-list prefix-list-name in [interface]
```

To delete a filter, use the `no distribute-list prefix-list-name in [interface]` command.

**Parameters**

- **prefix-list-name**: Enter the name of a configured prefix list.
- **interface**: (OPTIONAL) Enter one of the following keywords and slot/port or number information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For Port Channel groups, enter the keywords `port-channel` then a number.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

- `ROUTER OSPF`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

**S3048–ON**

**Syntax**

```
distribute-list prefix-list-name out [bgp | connected | isis | rip | static]
```

To remove a filter, use the `no distribute-list prefix-list-name out [bgp | connected | isis | rip | static]` command.

**Parameters**

- `prefix-list-name` Enter the name of a configured prefix list.
- `bgp` (OPTIONAL) Enter the keyword `bgp` to specify that BGP routes are distributed.
  
  ☑️ **NOTE:** BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.
- `connected` (OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.
- `isis` (OPTIONAL) Enter the keyword `isis` to specify that IS-IS routes are distributed.
  
  ☑️ **NOTE:** BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.
- `rip` (OPTIONAL) Enter the keyword `rip` to specify that RIP routes are distributed.
  
  ☑️ **NOTE:** BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.
- `static` (OPTIONAL) Enter the keyword `static` to specify that only manually configured routes are distributed.

**Defaults**

Not configured.

**Command Modes**

- ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Usage Information
The distribute-list out command applies to routes autonomous system boundary routers (ASBRs) redistribute 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.

S3048-ON

Syntax
fast-convergence {number}

To cancel fast-convergence, use the no fast convergence command.

Parameters
number
Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is from 1 to 4.

Defaults
None.

Command Modes
ROUTER OSPF

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the S9000.
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.
The higher this parameter is set, the faster OSPF converge takes place.

**NOTE:** The faster the convergence, the more frequent the route calculations and updates. This behavior impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking technical support.

**graceful-restart grace-period**

Specifies the time duration, in seconds, that the router’s neighbors continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

**NOTE:** This command enables OSPFv2 graceful restart globally by setting the grace period (in seconds) that an OSPFv2 router’s neighbors continues to advertise the router as adjacent during a graceful restart.

### S3048–ON

**Syntax**

```
graceful-restart grace-period seconds
```

To disable the grace period, use the `no graceful-restart grace-period` command.

**Parameters**

- **seconds**
  
  Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is from 40 to 1800 seconds.

**Defaults**

Not Configured

**Command Modes**

ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
Usage Information

The Helper mode is enabled by default on the device. To enable the restart mode also on the device, you must configure the grace period using this command. After you enable restart mode the router advertises the neighbor as fully adjacent during a restart.

**graceful-restart helper-reject**

Specify the OSPF router to not act as a helper during graceful restart.

**S3048-ON**

**Syntax**

```
graceful-restart helper-reject ip-address
```

To return to default value, use the `no graceful-restart helper-reject` command.

**Parameters**

- `ip-address` Enter the OSPF router-id, in IP address format, of the restart router that will not act as a helper during graceful restart.

**Defaults**

Not configured.

**Command Modes**

ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(1.0)
- 9.8(0.0P5)
- 9.8(0.0P2)
- 9.7(0.0)
- 9.2(1.0)
- 9.0.2.0
- 8.3.19.0
- 8.3.11.1
- 8.3.12.0
- 7.8.1.0

**Description**

- Introduced on the Z9100-ON.
- Introduced on the S4048-ON.
- Introduced on the S3048-ON.
- Introduced on the S6000-ON.
- Introduced on the Z9500.
- Introduced on the Z9000.
- Introduced on the S4820T.
- Introduced on the Z9000.
- Introduced on the S4810.

**Restart role enabled on the S-Series (Both Helper and Restart roles now supported on S-Series). Added support for Multi-Process OSPF.**
graceful-restart mode

Enable the graceful restart mode.

S3048-ON

Syntax
graceful-restart mode [planned-only | unplanned-only]
To disable graceful restart mode, use the no graceful-restart mode command.

Parameters
planned-only  (OPTIONAL) Enter the keywords planned-only to indicate graceful restart is supported in a planned restart condition only.
unplanned-only (OPTIONAL) Enter the keywords unplanned-only to indicate graceful restart is supported in an unplanned restart condition only.

Defaults
Support for both planned and unplanned failures.

Command Modes
ROUTER OSPF

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  Description
9.8(1.0)       Introduced on the Z9100-ON.
9.8(0.0P5)     Introduced on the S4048-ON.
9.8(0.0P2)     Introduced on the S3048-ON.
9.7(0.0)       Introduced on the S6000-ON.
9.2(1.0)       Introduced on the Z9500.
9.0.2.0        Introduced on the S6000.
8.3.19.0       Introduced on the S4820T.
8.3.11.1       Introduced on the Z9000.
8.3.12.0       Introduced on the S4810.
7.8.1.0        Introduced on the S-Series.
7.5.1.0        Introduced on the C-Series.
pre- 6.1.1.1   Introduced on the E-Series.
graceful-restart role

Specify the role for your OSPF router during graceful restart.

S3048-ON

Syntax

graceful-restart role [helper-only | restart-only]

To disable graceful restart role, use the no graceful-restart role command.

Parameters

role helper-only  (OPTIONAL) Enter the keywords helper-only to specify the OSPF router is a helper only during graceful restart.

role restart-only  (OPTIONAL) Enter the keywords restart-only to specify the OSPF router is a restart only during graceful-restart.

Defaults

By default, OSPF routers are both helper and restart routers during a graceful restart.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version     Description

9.8(1.0)     Introduced on the Z9100-ON.
9.8(0.0)     Introduced on the S3048-ON and S4048-ON.
9.7(0.0)     Introduced on the S6000-ON.
9.2(1.0)     Introduced on the Z9500.
9.0.2.0      Introduced on the S6000.
8.3.19.0     Introduced on the S4820T.
8.3.11.1     Introduced on the Z9000.
8.3.12.0     Introduced on the S4810.
7.8(1.0)     Added support for Multi-Process OSPF. Added Restart and Helper roles support on the S-Series.
7.7(1.0)     Added Helper-Role support on the S-Series.
7.5(1.0)     Introduced on the C-Series.
pre- 6.1.1.1  Introduced on the E-Series.
ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme until the grace period expires.

S3048-ON

Syntax

ip ospf auth-change-wait-time seconds

To return to the default, use the no ip ospf auth-change-wait-time command.

Parameters

seconds Enter the seconds. The range is from 0 to 300.

Defaults

zero (0) seconds.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

S3048-ON

Syntax

ip ospf authentication-key [encryption-type] key

To delete an authentication key, use the no ip ospf authentication-key command.
Parameters

- encryption-type (OPTIONAL) Enter 7 to encrypt the key.
- key Enter an eight-character string. Strings longer than eight characters are truncated.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.

Usage Information

All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

**S3048–ON**

Syntax

```
ip ospf cost cost
```

To return to default value, use the `no ip ospf cost` command.

Parameters

- cost Enter a number as the cost. The range is from 1 to 65535.

Defaults

The default cost is based on the reference bandwidth.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If this command is not configured, cost is based on the auto-cost command.

When you configure OSPF over multiple vendors, to ensure that all routers use the same cost, use the `ip ospf cost` command. Otherwise, OSPF routes improperly.

Related Commands

- `auto-cost` — control 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.

**S3048-ON**

**Syntax**

```
ip ospf dead-interval seconds
```

To return to the default values, use the `no ip ospf dead-interval` command.

**Parameters**

- **seconds**
  
Enter the number of seconds for the interval. The range is from 1 to 65535. The default is 40 seconds.

**Defaults**

40 seconds

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
Usage Information
By default, the dead interval is four times the default hello-interval.

Related Commands
• ip ospf hello-interval — set the time interval between the hello packets.

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

S3048–ON

Syntax
ip ospf hello-interval seconds
To return to the default value, use the no ip ospf hello-interval command.

Parameters
seconds
Enter the number of seconds for the interval. The range is from 1 to 65535. The default is 10 seconds.

Defaults
10 seconds

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.
**Usage Information**

The time interval between the hello packets must be the same for routers in a network.

**Related Commands**

- `ip ospf dead-interval` — set 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.

**Syntax**

```plaintext
ip ospf message-digest-key keyid md5 key
```

To delete a key, use the `no ip ospf message-digest-key keyid` command.

**Parameters**

- `keyid` Enter a number as the key ID. The range is from 1 to 255.
- `key` Enter a continuous character string as the password.

**Defaults**

No MD5 authentication is configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3(19.0) | Introduced on the S4820T.
8.3.11.0 | Introduced on the S4810.
8.3.10.0 | Introduced on the E-Series.
8.3.7.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.1 | Introduced on the E-Series.
Usage Information

You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. Dell Networking OS sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell recommends keeping only one key per interface.

**NOTE:** The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

**ip ospf mtu-ignore**

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

**S3048-ON**

**Syntax**

```
ip ospf mtu-ignore
```

To return to the default, use the `no ip ospf mtu-ignore` command.

**Defaults**

Enabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0) | Introduced on the S3048-ON and S4048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
**ip ospf network**

Set the network type for the interface.

### S3048-ON

**Syntax**

```
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the `no ip ospf network` command.

**Parameters**

- `broadcast` Enter the keyword `broadcast` to designate the interface as part of a broadcast network.
- `point-to-point` Enter the keywords `point-to-point` to designate the interface as part of a point-to-point network.

**Defaults**

Broadcast.

**Command Modes**

`ROUTER OSPF`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

**S3048-ON**

**Syntax**

```
ip ospf priority number
```

To return to the default setting, use the `no ip ospf priority` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Enter a number as the priority. The range is from 0 to 255. The default is 1.</td>
</tr>
</tbody>
</table>

**Defaults**

1

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.

S3048-ON

Syntax

ip ospf retransmit-interval seconds

To return to the default values, use the no ip ospf retransmit-interval command.

Parameters

seconds Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is 5 seconds.

This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults

5 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

pre-6.1.1.1 Introduced on the E-Series.

Usage Information

Set the time interval to a number large enough to prevent unnecessary retransmissions.
ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

S3048–ON

Syntax

```
ip ospf transmit-delay seconds
```

To return to the default value, use the `no ip ospf transmit-delay` command.

Parameters

- `seconds`
  - Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is 1 second.
  - This value must be greater than the transmission and propagation delays for the interface.

Defaults

- 1 second

Command Modes

- INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set Dell Networking OS.

S3048–ON

Syntax

```
log-adjacency-changes
```

Open Shortest Path First (OSPFv2 and OSPFv3) | 1029
To disable the Syslog messages, use the `no log-adjacency-changes` command.

### Defaults
Disabled.

### Command Modes
- ROUTER OSPF

### Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.7.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>10.7.0.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>10.3.19.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>10.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>10.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### maximum-paths
Enable the software to forward packets over multiple paths.

**S3048-ON**

```markdown
Syntax
maximum-paths number
```

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

**Parameters**
- `number` Specify the number of paths. The range for OSPFv2 is from 1 to 64. The default for OSPFv2 is **4 paths**. The range for OSPFv3 is from 1 to 64. The default for OSPFv3 is **8 paths**.

**Defaults**
4

**Command Modes**
- ROUTER OSPF for OSPFv2
- ROUTER OSPFv3 for OSPFv3

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

S3048–ON

Syntax

network ip-address mask area area-id

To disable an OSPF area, use the no network ip-address mask area area-id command.

Parameters

- **ip-address**: Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
- **mask**: Enter a network mask in /prefix format. (/x)
- **area-id**: Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is from 0 to 65535. IP address format is dotted decimal format A.B.C.D.

**NOTE**: If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.

Command Modes

- ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced to all platforms.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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.

**S3048-ON**

**Syntax**

```
passive-interface {default | interface}
```

To enable both the receiving and sending routing, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

**Parameters**

- **default**
  - Enter the keyword `default` to make all OSPF interfaces (current and future) passive.

- **interface**
  - Enter the following keywords and slot/port or number information:
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword ` TenGigabitEthernet` then the slot/port information.
    - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Command Modes**

- ROUTER OSPF
**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>74.1.0</td>
<td>Modified to include the keyword default.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent using other interfaces.

The **default** keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the no passive-interface interface command. The no form of this command is inserted into the configuration for individual interfaces when the no passive-interface interface command is issued while passive-interface default is configured.

This command behavior has changed as follows:

- **passive-interface interface**
  - The previous no passive-interface interface is removed from the running configuration.
  - The ABR status for the router is updated.
  - Save passive-interface interface into the running configuration.

- **passive-interface default**
  - All present and future OSPF interfaces are marked as passive.
  - Any adjacency is explicitly terminated from all OSPF interfaces.
  - All previous passive-interface interface commands are removed from the running configuration.
  - All previous no passive-interface interface commands are removed from the running configuration.

- **no passive-interface interface**
  - Remove the interface from the passive list.
  - The ABR status for the router is updated.
- If `passive-interface default` is specified, then save `no passive-interface interface` into the running configuration.

**No passive-interface default**

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

On configuring suppression using the `passive-interface` command, the state of the OSPF neighbor does not change to INIT; instead, the state of the OSPF neighbor changes to DOWN after the dead-timer expires.

**redistribute**

Redistribute information from another routing protocol throughout the OSPF process.

### S3048-ON

**Syntax**

```
redistribute {connected | isis | ospf | rip | static} [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute {connected | isis | rip | static}` command.

**Parameters**

- **connected**
  - Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.

- **isis**
  - Enter the keyword `isis` to specify that ISO IS-IS information is redistributed.

- **ospf**
  - Enter the keyword `ospf` to specify that information corresponding to OSPF is redistributed.

- **rip**
  - Enter the keyword `rip` to specify that RIP routing information is redistributed.

- **static**
  - Enter the keyword `static` to specify that information from static routes is redistributed.

- **metric metric-value**
  - (OPTIONAL) Enter the keyword `metric` then a number. The range is from 0 (zero) to 16777214.

- **metric-type type-value**
  - (OPTIONAL) Enter the keywords `metric-type` then one of the following:
    - 1 = OSPF External type 1
    - 2 = OSPF External type 2

- **route-map map-name**
  - (OPTIONAL) Enter the keywords `route-map` then the name of the route map.

- **tag tag-value**
  - (OPTIONAL) Enter the keyword `tag` then a number. The range is from 0 to 4294967295.

**Defaults**

Not configured.

**Command Modes**

- `ROUTER OSPF`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Added support for Multi-Process OSPF.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.

Usage Information
To redistribute the default route (0.0.0.0/0), configure the default-information originate command. Despite removing an OSPF process globally, the OSPF process is not completely removed from the BGP configuration.

Related Commands
- default-information originate — generate a default route into the OSPF routing domain.

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

S3048–ON

Syntax
redistribute bgp as number [metric metric-value] | [metric-type type-value] | [tag tag-value]

To disable redistribution, use the no redistribute bgp as number [metric metric-value] | [metric-type type-value] [route-map map-name] [tag tag-value] command.

Parameters
- as number Enter the autonomous system number. The range is from 1 to 65535.
- metric metric-value (OPTIONAL) Enter the keyword metric then the metric-value number. The range is from 0 to 16777214.
- metric-type type-value (OPTIONAL) Enter the keywords metric-type then one of the following:
  - 1 = for OSPF External type 1
  - 2 = for OSPF External type 2
- route-map map-name (OPTIONAL) Enter the keywords route-map then the name of the route map.
**redistribute isis**

Redistribute IS-IS routing information throughout the OSPF instance.

### S3048-ON

**Syntax**

```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]
```

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]` command.

**Parameters**

- **tag**
  - (OPTIONAL) Enter the name of the IS-IS routing process.

- **level-1**
  - (OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.

- **level-1-2**
  - (OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.

---

**Tag tag-value**

(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

**Defaults**

None

**Command Modes**

ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.3</td>
<td>Added Route Map for BGP Redistribution to OSPF.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added the keyword <code>default</code>.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
level-2 (OPTIONAL) Enter the keywords level-2 to redistribute only IS-IS Level-2 routes.

metric metric-value (OPTIONAL) Enter the keyword metric then a number. The range is from 0 (zero) to 4294967295.

metric-type type-value (OPTIONAL) Enter the keywords metric-type then one of the following:
  • 1 = for OSPF External type 1
  • 2 = for OSPF External type 2

route-map map-name (OPTIONAL) Enter the keywords route-map then the name of the route map.
tag tag-value (OPTIONAL) Enter the keyword tag to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Added support for Multi-Process OSPF.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.

router-id

To configure a fixed router ID, use this command.

S3048-ON

Syntax router-id ip-address

To remove the fixed router ID, use the no router-id ip-address command.
Parameters

**ip-address**
Enter the router ID in the IP address format.

Defaults

None.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

```plaintext
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.

**S3048–ON**

**Syntax**

```
routing ospf process-id
```
To clear an OSPF instance, use the `no router ospf process-id` command.

**Parameters**

`process-id`  
Enter a number for the OSPF instance. The range is from 1 to 65535.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Added support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF.

**Example**

```
Dell(conf)# router ospf 2
Dell(conf-router_ospf)#
```

---

**show config**

Display the non-default values in the current OSPF configuration.

**S3048-ON**

**Syntax**

```
show config
```

**Command Modes**

ROUTER OSPF

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**show ip ospf**

Display information on the OSPF process configured on the switch.

**S3048-ON**

**Syntax**

```
show ip ospf [process-id | vrf vrf name]
```

**Parameters**

- `process-id`  
  Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

- `vrf vrf name`  
  Show only the OSPF information tied to the VRF process.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**  

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
### Version Description

- **9.2(1.0)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.8.0** Added output for LSA throttling timers.
- **8.3.7.0** Added support for VRF.
- **7.9.1.0** Added support of Multi-Process OSPF.
- **7.8.1.0** Added the `process-id` option, in support of Multi-Process OSPF.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.
- **pre-6.1.1.1** Introduced on the E-Series.

### Usage Information

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the `show ip ospf` command shown in the following example.

<table>
<thead>
<tr>
<th>Line Beginning with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Routing Process...</em></td>
<td>Displays the OSPF process ID and the IP address associated with the process ID.</td>
</tr>
<tr>
<td><em>Supports only...</em></td>
<td>Displays the number of Type of Service (TOS) routes supported.</td>
</tr>
<tr>
<td><em>SPF schedule...</em></td>
<td>Displays the delay and hold time configured for this process ID.</td>
</tr>
<tr>
<td><em>Convergence Level</em></td>
<td>Displays the intervals set for LSA transmission and acceptance.</td>
</tr>
<tr>
<td><em>Min LSA...</em></td>
<td>Displays the number and type of areas configured for this process ID.</td>
</tr>
</tbody>
</table>

### 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
Dell#
```

### Related Commands
- `show ip ospf database` — display information about the OSPF routes configured.
- `show ip ospf interface` — display the OSPF interfaces configured.
- `show ip ospf neighbor` — display the OSPF neighbors configured.
show ip ospf asbr

Display all autonomous system boundary router (ASBR) routers visible to OSPF.

S3048-ON

Syntax
show ip ospf [process-id | vrf vrf-name] asbr

Parameters

- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults
None

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Added support of Multi-Process OSPF.
7.8.1.0 Added the process-id option, in support of Multi-Process OSPF.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series and E-Series.

Usage Information
To isolate problems with external routes, use this command. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

**NOTE:** ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the following example, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-).
show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

S3048-ON

Syntax

```
show ip ospf process-id [vrf vrf-name] database [database-summary]
```

Parameters

- **process-id**
  - Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **vrf vrf-name**
  - Enter the keyword `vrf` and then the name of the VRF to view LSA information on OSPF processes corresponding to that VRF.
- **database-summary**
  - (OPTIONAL) Enter the keywords `database-summary` to display the number of LSA types in each area and the total number of LSAs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support of Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
The following describes the `show ip ospf process-id database` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Identifies the router ID.</td>
</tr>
<tr>
<td>ADV Router</td>
<td>Identifies the advertising router's ID.</td>
</tr>
<tr>
<td>Age</td>
<td>Displays the link state age.</td>
</tr>
<tr>
<td>Seq#</td>
<td>Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA's complete contents.</td>
</tr>
<tr>
<td>Link count</td>
<td>Displays the number of interfaces for that router.</td>
</tr>
</tbody>
</table>

**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 0x80000006 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 0x8d8d   0
  13.1.1.0    13.1.1.1     1192 0x80000006 0x2718   0
  13.1.2.0    13.1.1.1     1184 0x80000006 0x1c22   0
  172.16.1.0  13.1.1.1     148  0x8000006d 0x533b   0

Dell>
```

**Related Commands**

- `show ip ospf database asbr-summary` — display only ASBR summary LSA information.

### show ip ospf database asbr-summary

Displays information about autonomous system (AS) boundary LSAs.

**S3048-ON**

**Syntax**

```
show ip ospf [process-id | vrf vrf-name] database asbr-summary [link-state-id] [adv-router ip-address]
```
Parameters

- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **link-state-id**: (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- **adv-router ip-address**: (OPTIONAL) Enter the keywords **adv-router** and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the **show ip ospf database asbr-summary** command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA’s age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
</tbody>
</table>
  - TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. |
  - DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. |
Field | Description
---|---
E or No E is displayed on whether the originating router can accept AS External LSAs.

LS Type | Displays the LSA’s type.
Link State ID | Displays the Link State ID.
Advertising Router | Identifies the advertising router’s ID.
Checksum | Displays the Fletcher checksum of the LSA’s complete contents.
Length | Displays the length in bytes of the LSA.
Network Mask | Displays the network mask implemented on the area.
TOS | Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric | Displays the LSA metric.

Example

Dell# show ip ospf 100 database asbr-summary

OSPF Router with ID (1.1.1.10) (Process ID 100)
Summary Asbr (Area 0.0.0.0)

LS age: 1437
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 103.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000000f
Checksum: 0x8221
Length: 28
Network Mask: /0
TOS: 0 Metric: 2

LS age: 473
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 104.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000010
Checksum: 0x4198
Length: 28
--More--

Related Commands
- `show ip ospf database` — display OSPF database information.

**show ip ospf database external**

Display information on the AS external (type 5) LSAs.

**Syntax**

```
show ip ospf [process-id] | vrf vrf-name] database external [link-state-id] [adv-router ip-address]
```

**Parameters**

- **process-id**
  - Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
**vrf vrf-name**

Enter the keyword `vrf` followed by the name of the VRF to view information on AS external LSAs corresponding to the OSPF processes that are tied to a specific VRF.

**link-state-id**

(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network’s IP address for Type 3 LSAs or Type 5 LSAs
- the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

**adv-router ip-address**

(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show ip ospf process-id database external` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA's age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td>- TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
<td></td>
</tr>
<tr>
<td>- DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
<td></td>
</tr>
<tr>
<td>- E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
<td></td>
</tr>
</tbody>
</table>
### Field Description
- **LS Type**: Displays the LSA’s type.
- **Link State ID**: Displays the Link State ID.
- **Advertising Router**: Identifies the router ID of the LSA’s originating router.
- **LS Seq Number**: Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
- **Checksum**: Displays the Fletcher checksum of the LSA’s complete contents.
- **Length**: Displays the length in bytes of the LSA.
- **Network Mask**: Displays the network mask implemented on the area.
- **Metrics Type**: Displays the external type.
- **TOS**: Displays the Type of Service (TOS) options. Option 0 is the only option.
- **Metric**: Displays the LSA metric.
- **Forward Address**: Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.
- **External Route Tag**: Displays the 32-bit field attached to each external route. The OSPF protocol does not use this field, but you can use the field for external route management.

### Example
```
Dell# show ip ospf 1 database external

OSPF Router with ID (20.20.20.5) (Process ID 1)
    Type-5 AS External
    LS age: 612
    Options: (No TOS-capability, No DC, E)
    LS type: Type-5 AS External
    Link State ID: 12.12.12.2
    Advertising Router: 20.31.3.1
    LS Seq Number: 0x80000007
    Checksum: 0x4cde
    Length: 36
    Network Mask: /32
        Metrics Type: 2
        TOS: 0
        Metrics: 25
        Forward Address: 0.0.0.0
        External Route Tag: 43

    LS age: 1868
    Options: (No TOS-capability, DC)
    LS type: Type-5 AS External
    Link State ID: 24.216.12.0
    Advertising Router: 20.20.20.8
    LS Seq Number: 0x80000005
    Checksum: 0xa00e
    Length: 36
    Network Mask: /24
        Metrics Type: 2
        TOS: 0
        Metrics: 1
        Forward Address: 0.0.0.0
        External Route Tag: 701

Dell#
```

### Related Commands
- `show ip ospf database` — display 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0(2.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show ip ospf process-id database network command shown in the following example.
Field  Description
LS Age  Displays the LSA's age.
Options  Displays the optional capabilities available on router. The following options can be found in this item:

- TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.
- DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.
- E or No E is displayed on whether the originating router can accept AS External LSAs.

LS Type  Displays the LSA's type.
Link State ID  Displays the Link State ID.
Advertising Router  Identifies the router ID of the LSA's originating router.
Checksum  Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length  Displays the Fletcher checksum of an LSA's complete contents.
Network Mask  Displays the length in bytes of the LSA.
Attached Router  Identifies the IP address of routers attached to the network.

Example

Dell# show ip ospf 1 data network
OSPF Router with ID (20.20.20.5) (Process ID 1)
Network (Area 0.0.0.0)
  LS age: 1372
  Options: (No TOS-capability, DC, E)
  LS type: Network
  Link State ID: 202.10.10.2
  Advertising Router: 20.20.20.8
  LS Seq Number: 0x80000006
  Checksum: 0xa35
  Length: 36
  Network Mask: /24
    Attached Router: 20.20.20.8
    Attached Router: 20.20.20.9
    Attached Router: 20.20.20.7

Network (Area 0.0.0.1)
  LS age: 252
  Options: (TOS-capability, No DC, E)
  LS type: Network
  Link State ID: 192.10.10.2
  Advertising Router: 192.10.10.2
  LS Seq Number: 0x80000007
  Checksum: 0x4309
  Length: 36
  Network Mask: /24
    Attached Router: 192.10.10.2
    Attached Router: 20.20.20.1
    Attached Router: 20.20.20.5

Dell#

Related Commands
- show ip ospf database — display OSPF database information.
show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

Syntax

```
show ip ospf [process-id | vrf vrf-name ] database nssa-external [link-state-id] [adv-router ip-address]
```

Parameters

- **process-id**
  - Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

- **vrf vrf-name**
  - Enter the keyword vrf followed by the name of the VRF to view NSSA-External LSA information corresponding to the OSPF process that is tied to a specific VRF.

- **link-state-id**
  - (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
    - the network’s IP address for Type 3 LSAs or Type 5 LSAs
    - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
    - the default destination (0.0.0.0) for Type 5 LSAs

- **adv-router ip-address**
  - (OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

Syntax

```
show ip ospf [process-id | vrf vrf-name] database opaque-area [link-state-id] [adv-router ip-address]
```

Parameters

- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **vrf vrf-name**: Enter the keyword vrf followed by the name of the VRF to view opaque-area LSA information corresponding to the OSPF process that is tied to a specific VRF.
- **link-state-id**: (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- **adv-router ip-address**: (OPTIONAL) Enter the keywords adv-router and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
### Version Description

- **8.3.7.0**: Introduced on the S4810.
- **7.8.1.0**: Added support for Multi-Process OSPF.
- **7.6.1.0**: Introduced on the S-Series.
- **7.5.1.0**: Introduced on the C-Series.
- **pre-6.1.1.1**: Introduced on the E-Series.

### Usage Information

The following describes the `show ip ospf process-id database opaque-area` command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA's age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>• TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>• DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>• E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA's type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the advertising router's ID.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of the LSA's complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Opaque Type</td>
<td>Displays the Opaque type field (the first 8 bits of the Link State ID).</td>
</tr>
<tr>
<td>Opaque ID</td>
<td>Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).</td>
</tr>
</tbody>
</table>

### 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--
```
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]
```

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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Added support for Multi-Process OSPF.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.1.1.1 | Introduced on the E-Series.

Related Commands

- **show ip ospf database** — display OSPF database information.
show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

Syntax

```
show ip ospf [process-id | vrf vrf-name] database opaque-link [link-state-id] [adv-router ip-address]
```

Parameters

- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- **vrf vrf-name**: Enter the keyword vrf followed by the name of the VRF to view opaque-link LSA information corresponding to the OSPF process that is tied to a specific VRF.
- **link-state-id** (OPTIONAL): Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- **adv-router ip-address** (OPTIONAL): Enter the keywords adv-router then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Version Description
pre-6.1.1.1 Introduced on the E-Series.

Related Commands
- show ip ospf database — display OSPF database information.

show ip ospf database router

Display the router (type 1) LSA information.

Syntax
show ip ospf [process-id | vrf vrf-name ] database router [link-state-id] [adv-router ip-address]

Parameters
- process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
- vrf vrf-name Enter the keyword vrf followed by the name of the VRF to view the router LSA information corresponding to the OSPF process that is tied to a specific VRF.
- link-state-id (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:
  - the network’s IP address for Type 3 LSAs or Type 5 LSAs
  - the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
  - the default destination (0.0.0.0) for Type 5 LSAs
- adv-router ip-address (OPTIONAL) Enter the keywords adv-router followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.20 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
### Version Description

- **7.8.1.0** Added support for Multi-Process OSPF.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.
- **pre-6.1.1.1** Introduced on the E-Series.

### Usage Information

The following describes the `show ip ospf process-id database router` command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>- TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>- DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>- E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA's originating router.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Displays the link state sequence number. This number detects duplicate or old LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA's complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
<tr>
<td>Number of Links</td>
<td>Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.</td>
</tr>
<tr>
<td>Link connected to:</td>
<td>Identifies the type of network to which the router is connected.</td>
</tr>
<tr>
<td>(Link ID)</td>
<td>Identifies the link type and address.</td>
</tr>
<tr>
<td>(Link Data)</td>
<td>Identifies the router interface address.</td>
</tr>
<tr>
<td>Number of TOS Metric</td>
<td>Lists the number of TOS metrics.</td>
</tr>
<tr>
<td>TOS 0 Metric</td>
<td>Lists the number of TOS 0 metrics.</td>
</tr>
</tbody>
</table>

### 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 Stub Network
(Link ID) Network/subnet number: 11.1.5.0

Related Commands
• show ip ospf database — display OSPF database information.

show ip ospf database summary

Display the network summary (type 3) LSA routing information.

Syntax
show ip ospf [process-id | vrf vrf-name] database summary [link-state-id] [adv-router ip-address]

Parameters
process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

vrf vrf-name Enter the keyword vrf followed by the name of the VRF to view LSA routing information corresponding to the OSPF process that is tied to a specific VRF.

link-state-id (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

• the network’s IP address for Type 3 LSAs or Type 5 LSAs
• the router’s OSPF router ID for Type 1 LSAs or Type 4 LSAs
• the default destination (0.0.0.0) for Type 5 LSAs
adv-router ip-address

(OPTIONAL) Enter the keywords adv-router then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show ip ospf process-id database summary command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Age</td>
<td>Displays the LSA age.</td>
</tr>
<tr>
<td>Options</td>
<td>Displays the optional capabilities available on router. The following options can be found in this item:</td>
</tr>
<tr>
<td></td>
<td>- TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service.</td>
</tr>
<tr>
<td></td>
<td>- DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits.</td>
</tr>
<tr>
<td></td>
<td>- E or No E is displayed on whether the originating router can accept AS External LSAs.</td>
</tr>
<tr>
<td>LS Type</td>
<td>Displays the LSA type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Displays the Link State ID.</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Identifies the router ID of the LSA’s originating router.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>Displays the Fletcher checksum of an LSA’s complete contents.</td>
</tr>
<tr>
<td>Length</td>
<td>Displays the length in bytes of the LSA.</td>
</tr>
</tbody>
</table>
### Item Description
- **Network Mask**: Displays the network mask implemented on the area.
- **TOS**: Displays the TOS options. Option 0 is the only option.
- **Metric**: Displays the LSA metrics.

### Example
```
Dell# show ip ospf 100 database summary

OSPF Router with ID (1.1.1.10) (Process ID 100)

    Summary Network (Area 0.0.0.0)
      LS age: 1551
      Options: (No TOS-capability, DC, E)
      LS type: Summary Network
      Link State ID: 192.68.16.0
      Advertising Router: 192.168.17.1
      LS Seq Number: 0x80000054
      Checksum: 0xb5a2
      Length: 28
      Network Mask: /24
        TOS: 0 Metric: 1

      LS age: 9
      Options: (No TOS-capability, No DC, E)
      LS type: Summary Network
      Link State ID: 192.68.32.0
      Advertising Router: 1.1.1.10
      LS Seq Number: 0x80000016
      Checksum: 0x987c
      Length: 28
      Network Mask: /24
        TOS: 0 Metric: 1

      LS age: 7
      Options: (No TOS-capability, No DC, E)
      LS type: Summary Network
      Link State ID: 192.68.33.0
      Advertising Router: 1.1.1.10
      LS Seq Number: 0x80000016
      Checksum: 0x1241
      Length: 28
      Network Mask: /26
        TOS: 0 Metric: 1

Dell#
```

### Related Commands
- `show ip ospf database` — display 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 | vrf vrf-name] interface [interface]
```

#### Parameters
- **process-id**: Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf vrf-name

Enter the keyword vrf followed by the name of the VRF to show the OSPF processes that are tied to a specific VRF.

interface

(OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4,(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the show ip ospf process-id interface command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</td>
<td>This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.</td>
</tr>
<tr>
<td>Internet Address...</td>
<td>This line displays the IP address, network mask and area assigned to this interface.</td>
</tr>
<tr>
<td>Process ID...</td>
<td>This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.</td>
</tr>
</tbody>
</table>
### Item | Description
---|---
Transmit Delay... | This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router... | This line displays the ID of the Designated Router and its interface address.
Backup Designated... | This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals... | This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due... | This line displays the amount time until the next Hello packet is sent out this interface.
Neighbor Count... | This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

#### Example

Dell> show ip ospf int

GigabitEthernet 1/7 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)

GigabitEthernet 1/8 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 | vrf vrf-name ] neighbor
```

#### Parameters

- `process-id` : Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
The command `show ip ospf vrf vrf-name` allows you to enter the keyword `vrf` followed by the name of the VRF to show information corresponding to the OSPF neighbors that are tied to a specific VRF.

**Command Modes**
- EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
The following describes the `show ip ospf process-id neighbor` command shown in the following example.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor ID</td>
<td>Displays the neighbor router ID.</td>
</tr>
<tr>
<td>Pri</td>
<td>Displays the priority assigned neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the OSPF state of the neighbor.</td>
</tr>
<tr>
<td>Dead Time</td>
<td>Displays the expected time until the Dell OS declares the neighbor dead.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the IP address of the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the interface type slot/port information.</td>
</tr>
<tr>
<td>Area</td>
<td>Displays the neighbor’s area (process ID).</td>
</tr>
</tbody>
</table>

**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 1/1 0.0.0.2
 192.10.10.2 1 FULL/DR     00:00:37 192.10.10.2 Gi 1/2 0.0.0.1
 20.20.20.1  1 FULL/DROTHER00:00:36 192.10.10.4 Gi 1/3 0.0.0.1
Dell#```

Open Shortest Path First (OSPFv2 and OSPFv3)  | 1063
show ip ospf routes

Display routes OSPF calculates and stores in OSPF RIB.

Syntax

```
show ip ospf [process-id | vrf vrf-name] routes
```

Parameters

- `process-id`
  - Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

- `vrf vrf-name`
  - Enter the keyword `vrf` followed by the name of the VRF to show the OSPF RIB information corresponding to the OSPF processes that are tied to a specific VRF.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series and E-Series.</td>
</tr>
</tbody>
</table>

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.
Starting with Version 9.4(0.0), the loopback IP address advertised to the neighbor is not displayed in the output because they are not accounted as inactive OSPF routes, whereas the loopback IP address is displayed until Dell Networking OS Version 9.3(0.0). Starting with Version 9.4(0.0), the `show ip ospf routes` command displays the interface and area ID information of connected networks in addition to the other settings, whereas these details are not displayed until Dell Networking OS Version 9.3(0.0). Starting with Version 9.4(0.0), the metric of E2 routes in the output is displayed as an external metric, whereas until Dell Networking OS Version 9.3(0.0), the number of hops to the ASBR for E2 routes are displayed in the output.

Example

```
Dell# show ip ospf 100 route
Prefix        Cost Nexthop   Interface Area  Type
1.1.1.1        1   0.0.0.0   Lo 0      0     Intra-Area
3.3.3.3        2   13.0.0.3  Gi 1/47   1     Intra-Area
13.0.0.0       1   0.0.0.0   Gi 1/47   0     Intra-Area
150.150.150.0  2   13.0.0.3  Gi 1/47   -     External
172.30.1.0     2   13.0.0.3  Gi 1/47   1     Intra-Area
Dell#
```

```
show ip ospf statistics
Display OSPF statistics.
```

Syntax

```
show ip ospf [process-id | vrf vrf-name] statistics global | [interface name {neighbor router-id}]
```

Parameters

- **process-id**
  
  Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

- **vrf vrf-name**
  
  Enter the keyword vrf followed by the name of the VRF to display statistics corresponding to the OSPF process that is tied to a specific VRF.

- **global**
  
  Enter the keyword global to display the packet counts received on all running OSPF interfaces and packet counts OSPF neighbors receive and transmit.

- **interface name**
  
  (OPTIONAL) Enter the keyword interface then one of the following interface keywords and slot/port or number information:

  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  
  - For a 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.

- **neighbor router-id**
  
  (OPTIONAL) Enter the keyword neighbor then the neighbor’s router-id in dotted decimal format (A,B,C,D).

Defaults

```
None
```

Command Modes

- EXEC
- EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

The following describes the show ip ospf statistics process-id global command shown in the following example.

<table>
<thead>
<tr>
<th>Row Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Displays the total number of packets the OSPF process receives/transmits.</td>
</tr>
<tr>
<td>Error</td>
<td>Displays the error count while receiving and transmitting packets by the OSPF process.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of OSPF Hello packets.</td>
</tr>
<tr>
<td>DDiscr</td>
<td>Number of database description packets.</td>
</tr>
<tr>
<td>LSRreq</td>
<td>Number of link state request packets.</td>
</tr>
<tr>
<td>LSUpd</td>
<td>Number of link state update packets.</td>
</tr>
<tr>
<td>LSAck</td>
<td>Number of link state acknowledgement packets.</td>
</tr>
<tr>
<td>TxQ-Len</td>
<td>The transmission queue length.</td>
</tr>
<tr>
<td>RxQ-Len</td>
<td>The reception queue length.</td>
</tr>
<tr>
<td>Tx-Mark</td>
<td>The highest number mark in the transmission queue.</td>
</tr>
<tr>
<td>Rx-Mark</td>
<td>The highest number mark in the reception queue.</td>
</tr>
<tr>
<td>Hello-Q</td>
<td>The queue, for transmission or reception, for the hello packets.</td>
</tr>
<tr>
<td>LSR-Q</td>
<td>The queue, for transmission or reception, for the link state request packets.</td>
</tr>
<tr>
<td>Other-Q</td>
<td>The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.</td>
</tr>
</tbody>
</table>

The following describes the error definitions for the show ip ospf statistics process-id global command.
<table>
<thead>
<tr>
<th>Error Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf_Down</td>
<td>Received packets on an interface that is either down or OSPF is not enabled.</td>
</tr>
<tr>
<td>Non-Dr</td>
<td>Received packets with a destination address of ALL_DRS even though SELF is not a designated router.</td>
</tr>
<tr>
<td>Self-Org</td>
<td>Receive the self originated packet.</td>
</tr>
<tr>
<td>Wrong_Len</td>
<td>The received packet length is different to what was indicated in the OSPF header.</td>
</tr>
<tr>
<td>Invl-Nbr</td>
<td>LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.</td>
</tr>
<tr>
<td>Nbr-State</td>
<td>LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.</td>
</tr>
<tr>
<td>Auth-Error</td>
<td>Simple authentication error.</td>
</tr>
<tr>
<td>MD5-Error</td>
<td>MD5 error</td>
</tr>
<tr>
<td>Chksum-Err</td>
<td>Checksum Error</td>
</tr>
<tr>
<td>Version</td>
<td>Version mismatch</td>
</tr>
<tr>
<td>AreaMismatch</td>
<td>Area mismatch</td>
</tr>
<tr>
<td>Conf-Issue</td>
<td>The received hello packet has a different hello or dead interval than the configuration.</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>Buffer allocation failure.</td>
</tr>
<tr>
<td>Seq-no</td>
<td>A sequence no errors occurred during the database exchange process.</td>
</tr>
<tr>
<td>Socket</td>
<td>Socket Read/Write operation error.</td>
</tr>
<tr>
<td>Q-overflow</td>
<td>Packets dropped due to queue overflow.</td>
</tr>
<tr>
<td>Unknown-Pkt</td>
<td>Received packet is not an OSPF packet.</td>
</tr>
</tbody>
</table>

Example

Dell# show ip ospf 1 statistics global

OSPF Packet Count

<table>
<thead>
<tr>
<th>Total Error</th>
<th>Hello</th>
<th>DDiscr</th>
<th>LSReq</th>
<th>LSUpd</th>
<th>LSAck</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX 10</td>
<td>0</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX 10</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

OSPF Global Queue Length

<table>
<thead>
<tr>
<th>Hello-Q</th>
<th>RxQ-Len</th>
<th>Tx-Mark</th>
<th>Rx-Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Error packets (Only for RX)

<table>
<thead>
<tr>
<th>Intf-Down</th>
<th>Non-Dr</th>
<th>Self-Org</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wrong-Len</td>
<td>Invl-Nbr</td>
<td>Nbr-State</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Auth-Err</td>
<td>MD5-Err</td>
<td>Chksum</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Version</td>
<td>AreaMis</td>
<td>Conf-Issues</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No-Buffer</td>
<td>Seq-No</td>
<td>Socket</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q-Overflow</td>
<td>Unkown-Pkt</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Error packets (Only for TX)

Socket Errors 0

Dell#

Usage Information

The show ip ospf process-id statistics command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
The grace-timer remaining value for each interface
The packet count received and transmitted for each neighbor
Dead timer remaining value for each neighbor
Transmit timer remaining value for each neighbor
The LSU Q length and its highest mark for each neighbor
The LSR Q length and its highest mark for each neighbor

Example (Statistics)

Dell(conf-if-gi-1/6)# do show ip ospf statistics
Interface GigabitEthernet 1/6
    Error packets (Receive statistics)
    Intf-Down 0 Non-Dr 0 Self-Org 0
    Wrong-Len 0 Invid-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 4.4.4.4
    Packet Statistics
    Hello DDiscr LSReq LSUpd LSAck
    RX 5 2 1 3 2
    TX 6 5 1 3 3
    Timers
    Hello 0 Wait 0 Grace 0
    Dead 39 Transmit 4
    Queue Statistics
    LSU-Q-Len 0 LSU-Q-Wmark 1
    LSR-Q-Len 0 LSR-Q-Wmark 1

Dell(conf-if-gi-1/6)#

Related Commands
  - clear ip ospf statistics — clear 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

Parameters
  - process-id

Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

Defaults
None

Command Modes
  - EXEC
  - EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

Example

Dell# show ip ospf 1 topology

Router ID  Flags  Cost  Nexthop   Interface Area
3.3.3.3    E/B/-/ 1    20.0.0.3  Gi 13/1   0
1.1.1.1    E/-/-/ 1    10.0.0.1  Gi 7/1    1
Dell#

summary-address

To advertise one external route, set the OSPF ASBR.

Syntax

summary-address ip-address mask [not-advertise] [tag tag-value]

To disable summary address, use the no summary-address ip-address mask command.

Parameters

- **ip-address**: Specify the IP address in dotted decimal format of the address to summarize.
- **mask**: Specify the mask in dotted decimal format of the address to summarize.
- **not-advertise**: (OPTIONAL) Enter the keywords not-advertise to suppress that match the network prefix/mask pair.
- **tag tag-value**: (OPTIONAL) Enter the keyword tag then a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
**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` — summarize 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.

**S3048-ON**

**Syntax**

```bash
timers spf delay holdtime
```

To return to the default, use the `no timers spf` command.

**Parameters**

- `delay` Enter a number as the delay. The range is from 0 to 4294967295. The default is 5 seconds.
- `holdtime` Enter a number as the hold time. The range is from 0 to 4294967295. The default is 10 seconds.

**Defaults**

- `delay = 5 seconds`
- `holdtime = 10 seconds`

**Command Modes**

- `ROUTER OSPF`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for Multi-Process OSPF.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Setting the `delay` and `holdtime` parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.

**Example**

```
Dell# conf
Dell(conf)# router ospf 1
Dell(conf-router_ospf-1)# timer spf 2 5
Dell(conf-router_ospf-1)# show config
!
router ospf 1
timers spf 2 5
Dell(conf-router_ospf-1)# end
```

**timers throttle lsa all**

Configure LSA transmit intervals.

**Syntax**

```
timers throttle lsa all {start-interval | hold-interval | max-interval}
```

To return to the default, use the `no timers throttle lsa` command.

**Parameters**

- `start-interval`
  - Set the minimum interval between initial sending and resending the same LSA. The range is from 0 to 600,000 milliseconds.

- `hold-interval`
  - Set the next interval to send the same LSA. This interval is the time between sending the same LSA after the start-interval has been attempted. The range is from 1 to 600,000 milliseconds.

- `max-interval`
  - Set the maximum amount of time the system waits before sending the LSA. The range is from 1 to 600,000 milliseconds.
Defaults

- start-interval: 0 msec
- hold-interval: 5000 msec
- max-interval: 5000 msec

Command Modes

- ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
## OSPFv3 Commands

Open shortest path first version 3 (OSPFv3) for IPv6 is supported on the S3048-ON platform.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

### area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OFSPFv3 area.

**Syntax**

```
area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key
```

**Parameters**

- **area area-id**
  - Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number.
  - The range is from 0 to 4294967295.

- **ipsec spi number**
  - Security Policy index (SPI) value that identifies an IPsec security policy.
  - The range is from 256 to 4294967295.

- **MD5 | SHA1**
  - Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).

- **key-encryption-type**
  - (OPTIONAL) Specifies if the key is encrypted.
  - The values are 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in authentication.
For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).

For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults
Not configured.

Command Modes
ROUTER OSPFv3

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.1(0.0) Introduced on the S4810 and Z9000.
8.3.19.0 Introduced on the S4820T.
8.4.2.0 Introduced on the E-Series.

Usage Information
Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFv3 area with the area encryption command, you cannot use the area authentication command in the area at the same time.

The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

To remove an IPsec authentication policy from an OSPFv3 area, enter the no area area-id authentication spi number command.

Related Commands
- ipv6 ospf authentication — configure an IPsec authentication policy on an OSPFv3 interface.
- show crypto ipsec policy — display the configuration of IPsec authentication policies.

area encryption

Configure an IPsec encryption policy for OSPFV3 packets in an OSPFV3 area.

Syntax
area area-id encryption ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key
Parameters

- **area area-id**
  
  Area for which OSPFv3 traffic is to be encrypted. For area-id, enter a number.
  
  The range is from 0 to 4294967295.

- **ipsec spi number**
  
  Security Policy index (SPI) value that identifies an IPsec security policy.
  
  The range is from 256 to 4294967295.

- **esp encryption-algorithm**
  
  Encryption algorithm used with ESP.
  
  Valid values are: 3DES, DES, AES-CBC, and NULL.
  
  For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

- **key-encryption-algorithm**
  
  (OPTIONAL) Specifies if the key is encrypted.
  
  Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  
  Text string used in encryption.

  The required lengths of a non-encrypted or encrypted key are:
  
  - 3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.

- **authentication-algorithm**
  
  Specifies the authentication algorithm to use for encryption.
  
  Valid values are MD5 or SHA1.

- **key-encryption-type**
  
  (OPTIONAL) Specifies if the authentication key is encrypted.
  
  Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  
  Text string used in authentication.

  For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).

  For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

- **null**
  
  Causes an encryption policy configured for the area to not be inherited on the interface.

**Defaults**

Not configured.

**Command Modes**

ROUTER OSPFv3

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
### auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

**S3048-ON**

**Syntax**

```plaintext
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
clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

Syntax

```plaintext
clear ipv6 ospf [vrf vrf-name] process
```

Parameters

- `vrf vrf-name`  
  (Optional) Enter the keyword vrf followed by the name of the VRF to clear IPv6 routes corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
debug ipv6 ospf bfd

Display debug information and interface types for bidirectional forwarding detection (BFD) on OSPF IPv6 packets.

Syntax

[no] debug ipv6 ospf bfd [interface]

Parameters

interface

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(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.
9.2.(0.0) Introduced on the S4820T, S4810, and Z9000.

Usage Information

The following section describes the command fields.

Lines Beginning With or Including

OSPFv3... Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01 Displays the time stamp.
Sending Ver:3 Sending OSPFv3 version..

Example

Dell(conf-if-gi-1/2)# do debug ipv6 ospf bfd gi 1/2
OSPFv3 bfd related debugging is on for GigabitEthernet 1/2
00:59:26 : OSPFv3INFO: Received Interface mode bfd config command on interface Gi 1/2 Enable 1, interval 0, min_rx 0, Multiplier 0, role 0, Disable 0
00:59:26 : OSPFv3INFO: Enabling BFD on interface Gi 1/2 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 Gi 1/2!!
00:59:27 : OSPFv3INFO: Completed Interface mode BFD configuration on Gi 1/2!!
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 Gi 1/2 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 11:20:00: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed session state to Up for neighbor fe80::201:e8ff:fe8b:7720 on interface Gi 1/2 (diag: NO_DIAG)
00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg
00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Gi 1/2
00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state

debug ipv6 ospf packet

Display debug information and interface types on OSPF IPv6 packets.

Syntax

debug ipv6 ospf {packet | events} [interface]

Parameters

interface

(OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on E-Series.</td>
</tr>
</tbody>
</table>
Example

Dell# debug ipv6 ospf packet
OSPFv3 packet related debugging is on for all interfaces
05:21:01 : OSPFv3: Sending, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.254, Area ID:0, Inst:0, on Po 255
05:21:03 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.255, Area ID:0, Chksum:a177, Inst:0, from Vl 100
05:20:25 : OSPFv3: Sending, Ver:3, Type:4(LS Update), Len:580, Router ID:223.255.255.254, Area ID:0, Inst:0, on Vl 1000
07:21:40 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:223.255.255.254, Area ID:0, Chksum:af8f, Inst:0, from Gi 1/6
Dell#

Command Fields

<table>
<thead>
<tr>
<th>Lines Beginning With or Including</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3...</td>
<td>Debugging is on for all OSPFv3 packets and all interfaces.</td>
</tr>
<tr>
<td>05:21:01</td>
<td>Displays the time stamp.</td>
</tr>
<tr>
<td>Sending Ver:3</td>
<td>Sending OSPF3 version..</td>
</tr>
<tr>
<td>type:</td>
<td>Displays the type of packet sent:</td>
</tr>
<tr>
<td>• 1 - Hello packet</td>
<td></td>
</tr>
<tr>
<td>• 2 - database description</td>
<td></td>
</tr>
<tr>
<td>• 3 - link state request</td>
<td></td>
</tr>
<tr>
<td>• 4 - link state update</td>
<td></td>
</tr>
<tr>
<td>• 5 - link state acknowledgement</td>
<td></td>
</tr>
<tr>
<td>• 7 - external LSA</td>
<td></td>
</tr>
<tr>
<td>• 8 - link-state advertisement (OSPFv3)</td>
<td></td>
</tr>
<tr>
<td>• 9 - link local LSA (OSPFv2), Intra-Area-Prefix LSA (OSPFv3)</td>
<td></td>
</tr>
<tr>
<td>• 11 - grace LSA (OSPFv3)</td>
<td></td>
</tr>
<tr>
<td>Length:</td>
<td>Displays the packet length.</td>
</tr>
<tr>
<td>Router ID:</td>
<td>Displays the OSPF3 router ID.</td>
</tr>
<tr>
<td>Area ID:</td>
<td>Displays the Area ID.</td>
</tr>
<tr>
<td>Chksum:</td>
<td>Displays the OSPF3 checksum.</td>
</tr>
</tbody>
</table>

default-information originate

Configure the Dell Networking OS to generate a default external route into an OSPFv3 routing domain.

Syntax

```
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

To return to the default values, use the no default-information originate command.

Parameters

- **always** (OPTIONAL) Enter the keyword always to specify that default route information must always be advertised.
- **metric metric-value** (OPTIONAL) Enter the keyword metric then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type

(Optional) Enter the keywords metric-type then an OSPFv3 link state type of 1 or 2 for default routes. The values are:

- 1 = Type 1 external route
- 2 = Type 2 external route

route-map

(Optional) Enter the keywords route-map then the name of an established route map.

Defaults

Disabled.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.1(0.0) Introduced on the S4810 and Z9000.
8.3.19.0 Introduced on the S4820T.
7.8.1.0 Added support for C-Series.
7.4.1.0 Introduced on the E-Series.

Related Commands

- redistribute — redistribute routes from other routing protocols into OSPFv3.

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router’s neighbors continues to advertise the router as adjacent during a graceful restart.

Syntax

graceful-restart grace-period seconds

To disable OSPFv3 graceful restart, enter no graceful-restart grace-period.

Parameters

- seconds Time duration, in seconds, that specifies the duration of the restart process before OSPFv3 terminates the process. The range is from 40 to 1800 seconds.

Defaults

OSPFv3 graceful restart is disabled and functions in a helper-only role.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.
**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.

**Syntax**

```
graceful-restart mode {planned-only | unplanned-only}
```

To disable graceful restart mode, enter `no graceful-restart mode`.

**Parameters**

- `planned-only`  
  
  (OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.

- `unplanned-only`  
  
  (OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

**Defaults**

OSPFv3 graceful restart supports both planned and unplanned failures.

**Command Modes**

```
ROUTER OSPFv3
```

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

```
9.8(1.0)  Introduced on the Z9100-ON.
9.8(0.0P5)  Introduced on the S4048-ON.
```

**Description**

```
Introduced on the Z9100-ON.
Introduced on the S4048-ON.
```
**ipv6 ospf area**

Enable IPv6 OSPF on an interface.

**Syntax**

```
ipv6 ospf process id area area-id
```

**Parameters**

- `process-id`  
  Enter the process identification number.

- `area area-id`  
  Specify the OSPF area. The range is from 0 to 65535.

**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**  

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
**ipv6 ospf authentication**

Configure an IPsec authentication policy for OSPFv3 packets on an IPv6 interface.

**Syntax**

```plaintext
ipv6 ospf authentication {null | ipsec spi number (MD5 | SHA1) [key-encryption-type] key}
```

**Parameters**

- **null**
  - Causes an authentication policy configured for the area to not be inherited on the interface.

- **ipsec spi number**
  - Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.

- **MD5 | SHA1**
  - Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).

- **key-encryption-type** (OPTIONAL)
  - Specifies if the key is encrypted.
  - Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

- **key**
  - Text string used in authentication.
  - For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).
  - For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

**Defaults**

- Not configured.

**Command Modes**

- INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on S4810 and Z9000.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec authentication policy from an interface, enter the no ipv6 ospf authentication spi number command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the no ipv6 ospf authentication null command.

**Related Commands**
- `area authentication` — configure an IPsec authentication policy for an OSPFv3 area.
- `show crypto ipsec policy` — display the configuration of IPsec authentication policies.
- `show crypto ipsec sa ipv6` — display the security associations set up for OSPFv3 interfaces in authentication policies.

**ipv6 ospf bfd all-neighbors**

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

**Syntax**

```
ipv6 ospf bfd all-neighbors [disable | [interval interval min_rx min_rx multiplier value role {active | passive}]]
```

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command in interface mode.

**Parameters**

- **disable**  
  (OPTIONAL) Enter the keyword disable to disable BFD on this interface.

- **interval milliseconds**  
  (OPTIONAL) Enter the keyword interval to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 200.

- **min_rx milliseconds**  
  Enter the keywords min_rx to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is 200.

- **multiplier value**  
  Enter the keyword multiplier to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is 3.

- **role [active | passive]**  
  Enter the role that the local system assumes:
  - **Active** — active system initiates the BFD session. Both systems can be active for the same session.
  - **Passive** — passive system does not initiate a session. It only responds to a request for session initialization from the active system.

  The default is Active.

**Defaults**

See Parameters.

**Command Modes**  
`INTERFACE`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure ipv6 ospf BFD in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the bfd all-neighbors command. Using the no form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword disable.

ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

Syntax

ipv6 ospf interface-cost

Parameters

interface-cost

Enter a unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults

Default cost based on the bandwidth.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

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.

7.8.1.0 Added support for C-Series.

7.4.1.0 Introduced on the E-Series.

8.3.19.0 Introduced on the S4820T.

Usage Information

In general, the path cost is calculated as:

1087
Using this formula, the default path cost is calculated as:

- GigabitEthernet — Default cost is 1
- 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**

```plaintext
ipv6 ospf dead-interval seconds
```

To return to the default time interval, use the `no ipv6 ospf dead-interval` command.

**Parameters**

- `seconds` Enter the time interval in seconds. The range is from 1 to 65535 seconds.

**Defaults**

40 seconds (Ethernet).

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, the dead interval is four times longer than the default hello-interval.

**Related Commands**

- `ipv6 ospf hello-interval` — specify the time interval between hello packets.
ipv6 ospf encryption

Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

Syntax
ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key [authentication-algorithm [key-encryption-type] key]}

Parameters
null
Causes an encryption policy configured for the area to not be inherited on the interface.

ipsec spi number
Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.

esp encryption-algorithm
Encryption algorithm used with ESP.
Valid values are: 3DES, DES, AES-CBC, and NULL.
For AES-CBC, only the AES-128 and AES-192 ciphers are supported.

key-encryption-type
(OPTIONAL) Specifies if the key is encrypted.
Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

key
Text string used in authentication.
The required lengths of a non-encrypted or encrypted key are:
3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC - 32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.

authentication-algorithm
Specifies the authentication algorithm to use for encryption. Valid values are MD5 or SHA1.

digest algorithm
(OPTIONAL) Specifies if the authentication key is encrypted.
Valid values: 0 (key is not encrypted) or 7 (key is encrypted).

key
Text string used in authentication.
For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).
For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults
Not configured.

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**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**

```plaintext
ipv6 ospf graceful-restart helper-reject
```

To disable the helper-reject role, enter `no ipv6 ospf graceful-restart helper-reject`.

**Defaults**

The helper-reject role is not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**     | **Description**                      
----------------|--------------------------------------
9.8(1.0)        | Introduced on the Z9100-ON.          
9.8(0.0P5)      | Introduced on the S4048-ON.          
9.8(0.0P2)      | Introduced on the S3048-ON.          
9.2(1.0)        | Introduced on the Z9500.             
9.1(0.0)        | Introduced on the S4810 and Z9000.   
8.4.2.0         | Introduced on the E-Series.          
8.3.19.0        | Introduced on the S4820T.            

**Before you enable IPsec encryption on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.**

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same encryption policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec encryption policy from an interface, enter the `no ipv6 ospf encryption spi` number command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFV3 area, enter the `no ipv6 ospf no ipv6 ospf encryption null` command.

**Related Commands**

- `area encryption` — configure an IPsec encryption policy for an OSPFv3 area.
- `show crypto ipsec policy` — display the configuration of IPsec encryption policies.
- `show crypto ipsec sa ipv6` — display the security associations set up for OSPFv3 interfaces in encryption policies.
## ipv6 ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

**Syntax**

```
ipv6 ospf hello-interval seconds
```

To return to the default time interval, enter **no ipv6 ospf hello-interval**.

**Parameters**

- `seconds` Enter the time interval in seconds as the time between hello packets. The range is from 1 to 65525 seconds.

**Defaults**

10 seconds (Ethernet).

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

**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.

Syntax

```
ipv6 ospf priority number
```

To return to the default time interval, use the `no ipv6 ospf priority` command.

Parameters

- `number`: Enter the number as the priority. The range is from 1 to 255.

Defaults

1

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ipv6 router ospf

Enable OSPF for IPv6 router configuration.

Syntax

```
ipv6 router ospf process-id [vrf vrf-name]
```
To exit OSPF for IPv6, use the no ipv6 router ospf process-id command.

Parameters

- **process-id**
  - Enter the process identification number. The range is from 1 to 65535.

- **vrf vrf-name**
  - (Optional) Enter the keyword vrf followed by the name of the VRF to install IPv6 routes in that VRF.

Defaults

- None

Command Modes

- CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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 is from 1 to 64. The default is 8 paths.

Defaults

- 8

Command Modes

- ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
passive-interface

Disable (suppress) sending routing updates on an interface.

Syntax

passive-interface interface

To enable sending routing updates on an interface, use the no passive-interface interface command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults

Enabled, that is sending of routing updates are enabled by default.

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.1(0.0) Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Added support for Multi-Process OSPF.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.1 Introduced on the E-Series.
Usage Information

By default, no interfaces are passive. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

On configuring suppression using the passive-interface command, the state of the OSPF neighbor does not change to INIT; instead, the state of the OSPF neighbor changes to DOWN after the dead-timer expires.

redistribute

Redistribute into OSPFv3.

Syntax

redistribute {bgp as number}{connected | static}[metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]

To disable redistribution, use the no redistribute {connected | static} command.

Parameters

bgp as number

Enter the keyword bgp then the autonomous system number.

The range is from 1 to 65535.

connected

Enter the keyword connected to redistribute routes from physically connected interfaces.

static

Enter the keyword static to redistribute manually configured routes.

metric metric-value

Enter the keyword metric then the metric value.

The range is from 0 to 16777214.

The default is 20.

metric-type type-value

(Optional) Enter the keywords metric-type then the OSPFv3 link state type of 1 or 2 for default routes. The values are:

- 1 for a type 1 external route
- 2 for a type 2 external route
The default is 2.

route-map map-name

(Optional) Enter the keywords route-map then the name of an established route map. If the route map is not configured, the default is deny (to drop all routes).

tag tag-value

(Optional) Enter the keyword tag to set the tag for routes redistributed into OSPFv3.

The range is from 0 to 4294967295

The default is 0.

Defaults
Not configured.

Command Modes
ROUTER OSPF for OSPFv2
ROUTER OSPFv3 for OSPFv3

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
To redistribute the default route (x:x:x:x::x), use the default-information originate command.

Related Commands
- default-information originate — configure default external route into OSPFv3.

router-id

Designate a fixed router ID.

Syntax
router-id ip-address

To return to the previous router ID, use the no router-id ip-address command.
Parameters

- **ip-address**: Enter the router ID in the dotted decimal format.

Defaults

- The router ID is selected automatically from the set of IPv4 addresses configured on a router.

Command Modes

- ROUTER OSPF for OSPFv2
- ROUTER OSPFv3 for OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1.(0.0)</td>
<td>Introduced support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.

If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.

Related Commands

- `clear ipv6 ospf process` — reset an OSPFv3 router process.

**show crypto ipsec policy**

Display the configuration of IPsec authentication and encryption policies.

Syntax

```
show crypto ipsec policy [name name]
```

Parameters

- **name name**: (OPTIONAL) Displays configuration details about a specified policy.

Defaults

- No default behavior or values.

Command Modes

- EXEC
- EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

- **9.8(1.0)** Introduced on the Z9100-ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.2(1.0)** Introduced on the Z9500.
- **8.1.(0.0)** Introduced on the S4810 and Z9000.
- **8.4.2.0** Introduced on the E-Series.
- **8.3.19.0** Introduced on the S4820T.

### Usage Information

The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

### Related Commands

- `show crypto ipsec sa ipv6`—displays the IPsec security associations used on OSPFv3 interfaces.

### Example

```
Dell# show crypto ipsec policy
Crypto IPsec client security policy data
Policy name : OSPFv3-1-502
Policy refcount : 1
Inbound ESP SPI : 502 (0x1F6)
Outbound ESP SPI : 502 (0x1F6)
Inbound ESP Auth Key : 123456789a123456789b123456789c12
Outbound ESP Auth Key : 123456789a123456789b123456789c12
Inbound ESP Cipher Key :
Outbound ESP Cipher Key :
Transform set : esp-3des esp-md5-hmac

Crypto IPsec client security policy data
Policy name : OSPFv3-0-501
Policy refcount : 1
Inbound ESP SPI : 501 (0x1F5)
Outbound ESP SPI : 501 (0x1F5)
Inbound ESP Auth Key :
Outbound ESP Auth Key :
Inbound ESP Cipher Key :
Outbound ESP Cipher Key :
Transform set : esp-128-aes esp-shal-hmac
```

1098 | Open Shortest Path First (OSPFv2 and OSPFv3)
### show crypto ipsec policy Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Displays the name of an IPsec policy.</td>
</tr>
<tr>
<td>Policy refcount</td>
<td>Number of interfaces on the router that use the policy.</td>
</tr>
<tr>
<td>Inbound ESP SPI and Outbound ESP SPI</td>
<td>The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.</td>
</tr>
<tr>
<td>Inbound ESP Auth Key and Outbound Auth Key</td>
<td>The ESP authentication key for inbound and outbound links.</td>
</tr>
<tr>
<td>Inbound ESP Cipher Key and Outbound ESP Cipher Key</td>
<td>The ESP encryption key for inbound and outbound links.</td>
</tr>
<tr>
<td>Transform set</td>
<td>The set of security protocols and algorithms used in the policy.</td>
</tr>
<tr>
<td>Inbound AH SPI and Outbound AH SPI</td>
<td>The authentication header (AH) security policy index (SPI) for inbound and outbound links.</td>
</tr>
<tr>
<td>Inbound AH Key and Outbound AH Key</td>
<td>The AH key for inbound and outbound links.</td>
</tr>
</tbody>
</table>

### show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

**Syntax**

```
show crypto ipsec sa ipv6 [interface interface]
```

**Parameters**

`interface interface` *(OPTIONAL)* Displays information about the SAs used on a specified OSPFv3 interface, where `interface` is one of the following values:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

**Defaults**

No default behavior or values.

**Command Modes**

EXEC

EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>

### Usage Information

The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

### Related Commands

- `show crypto ipsec policy` — displays the configuration of IPsec authentication and encryption policies.

### Example

```
Dell# show crypto ipsec policy
Dell# show crypto ipsec sa ipv6

Interface: GigabitEthernet 1/1
Link Local address: fe80::201:e8ff:fe40:4d10
IPSecv6 policy name: OSPFv3-1-500

inbound ah sas
spi : 500 (0x1f4)
   transform : ah-md5-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE

outbound ah sas
spi : 500 (0x1f4)
   transform : ah-md5-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE

inbound esp sas
outbound esp sas

Interface: GigabitEthernet 1/2
Link Local address: fe80::201:e8ff:fe40:4d11
IPSecv6 policy name: OSPFv3-1-600

inbound ah sas
outbound ah sas

inbound esp sas
spi : 600 (0x258)
   transform : esp-des esp-sha1-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE

outbound esp sas
```
show crypto ipsec sa ipv6 Command Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>IPv6 interface</td>
</tr>
<tr>
<td>Link local address</td>
<td>IPv6 address of interface</td>
</tr>
<tr>
<td>IPSecv6 policy name</td>
<td>Name of the IPsec security policy applied to the interface.</td>
</tr>
<tr>
<td>inbound/outbound</td>
<td>Authentication policy applied to inbound or outbound traffic.</td>
</tr>
<tr>
<td>ah</td>
<td>Encryption policy applied to inbound or outbound traffic.</td>
</tr>
<tr>
<td>spi</td>
<td>Security policy index number used to identify the policy.</td>
</tr>
<tr>
<td>transform</td>
<td>Security algorithm that is used to provide authentication, integrity, and confidentiality.</td>
</tr>
<tr>
<td>in use settings</td>
<td>Transform that the SA uses (only transport mode is supported).</td>
</tr>
<tr>
<td>replay detection</td>
<td>Y: An SA has enabled the replay detection feature.</td>
</tr>
<tr>
<td>support</td>
<td>N: The replay detection feature is not enabled.</td>
</tr>
<tr>
<td>STATUS</td>
<td>ACTIVE: The authentication or encryption policy is enabled on the interface.</td>
</tr>
</tbody>
</table>

show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

Syntax

```
show ipv6 ospf [process-number] [vrf vrf-name] database [database-summary | grace-lsa]
```

Parameters

- **process-number**: Enter the OSPF process number.
- **vrf vrf-name**: (Optional) Enter the keyword vrf followed by the name of the VRF to display neighbors corresponding to that VRF.
  
  - **NOTE**: If you do not specify this option, neighbors corresponding to the default VRF are displayed.

- **database-summary**: (OPTIONAL) Enter the keywords database-summary to view a summary of database LSA information.
grace-lsa

(Optional): Enter the keywords grace-lsa to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.

Defaults
None

Command Modes
EXEC

EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Added support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.4.2.2</td>
<td>Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series routers.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The show crypto ipsec sa ipv6 command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

Related Commands
show crypto ipsec policy — displays the configuration of IPsec authentication and encryption policies.

Example (grace-lsa)
Dell# show ipv6 ospf 3 database grace-lsa
Type-11 Grace LSA (Area 0)

  LS Age : 10
  Link State ID : 6.16.192.66
  Advertising Router : 100.1.1.1
  LS Seq Number : 0x80000001
  Checksum : 0x1DF1
  Length : 36
  Associated Interface : Gi 1/3
  Restart Interval : 180
  Restart Reason : Switch to Redundant Processor

Example (database-summary)
Dell# show ipv6 ospf 3 database database-summary
OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

  Process 1 database summary
  Type Count/Status
  Oper Status 1
  Admin Status 1
  Area Bdr Rtr Status 1
  AS Bdr Rtr Status 1
  AS Scope LSA Count 0
  AS Scope LSA Cksum sum 0
show ipv6 ospf interface

View OSPFv3 interface information.

Syntax

show ipv6 ospf [process-number] [vrf vrf-name] [interface]

Parameters

process-number

Enter the OSPF process number.

vrf vrf-name

(Optional) Enter the keyword vrf followed by the name of the VRF to display neighbors corresponding to that VRF.

NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.

interface

(Optional) Enter one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
For a port channel interface, enter the keywords *port-channel* then a number.

For a VLAN interface, enter the keyword *vlan* then a number from 1 to 4094.

**Defaults**

None

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(10)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Added support for showing BFD status on the S4820T, S4810, and Z9000.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Added support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you enable BFD at the global level, *show ipv6 ospf interface* shows the BFD provisioning.

If you enable BFD at the interface level, *show ipv6 ospf interface* shows the BFD interval timers.

**Example**

```
Dell# show ipv6 ospf 3 interface gigabitethernet 1/2

GigabitEthernet 1/2 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Interface is using OSPF global mode BFD configuration.
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5

Dell#
```

**show ipv6 ospf neighbor**

Display the OSPF neighbor information on a per-interface basis.

**Syntax**

```
show ipv6 ospf [process-number] [vrf vrf-name] neighbor [interface]
```

**Parameters**

- `process-number` : Enter the OSPF process number.
vrf vrf-name

(Optional) Enter the keyword vrf followed by the name of the VRF to display OSPF neighbors corresponding to that VRF.

**NOTE:** If you do not specify this option, neighbors corresponding to the default VRF are displayed.

**Interface**

(Optional) Enter the following keywords and the interface 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.

**Defaults**

None

**Command Modes**

EXEC

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced support for OSPFv3 on the S4810 and Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Added support for the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ipv6 ospf 3 neighbor gi 1/2
Neighbor ID  Pri   State       Dead Time   Interface   ID Interface
63.114.8.36  1   FULL/DR   00:00:38       4               Gi 1/2
Dell#
```

**timers spf**

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

**S3048-ON**

**Syntax**

```
timers spf delay holdtime
```

To return to the default, use the no timers spf command.
Parameters

- **delay**
  
  Enter a number as the delay. The range is from 0 to 4294967295. The default is 5 seconds.

- **holdtime**
  
  Enter a number as the hold time. The range is from 0 to 4294967295. The default is 10 seconds.

Defaults

- delay = 5 seconds
- holdtime = 10 seconds

Command Modes

- **ROUTER OSPFv3 for OSPFv3**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S6000-ON, S6000, S4820T, S4810, S5000.</td>
</tr>
</tbody>
</table>

Usage Information

Setting the delay and holdtime parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.

Example

```
Dell# conf
Dell(conf)# ipv6 router ospf 1
Dell(conf-ipv6-router_ospf)# timer spf 2 5
Dell(conf-ipv6-router_ospf)# show config
!
ipv6 router ospf 1
timers spf 2 5
Dell(conf-ipv6-router_ospf)#
Dell(conf-ipv6-router_ospf)# end
Dell#
```
Policy-based Routing (PBR)

Policy-based routing (PBR) allows you to apply routing policies to specific interfaces. To enable PBR, create a redirect list and apply it to the interface. After the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list. PBR is supported by the Dell Networking 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.

1. **NOTE:** Apply PBR to Layer 3 interfaces only.
2. **NOTE:** For more information, see Content Addressable Memory (CAM).

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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
**ip redirect-group**

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

**Syntax**

```
ip redirect-group redirect-list-name
```

To remove a redirect list from an interface, use the `no ip redirect-group name` command.

**Parameters**

- `redirect-list-name` Enter the name of a configured redirect list.

**Defaults**

None

**Command Modes**

INTERFACE (conf-if-vl-)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can apply any number of redirect-groups to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.
If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise, the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

**NOTE:** Apply the redirect list to physical, VLAN, or LAG interfaces only.

Related Commands
- `show cam pbr` – display the content of the PBR CAM.
- `show ip redirect-list` – display 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

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>8.4.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>6.5.3.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
**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.

**Parameters**

- **ip-protocol-number**: Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
- **protocol-type**: Enter one of the following keywords as the protocol type:
  - `icmp` for internet control message protocol
  - `ip` for any internet protocol
  - `tcp` for transmission control protocol
  - `udp` for user datagram protocol
- **source**: Enter the IP address of the network or host from which the packets were sent.
- **mask**: Enter a network mask in /prefix format (/x).
- **any**: Enter the keyword `any` to specify that all traffic is subject to the filter.
- **host ip-address**: Enter the keyword `host` then the IP address to specify a host IP address.
- **destination**: Enter the IP address of the network or host to which the packets are sent.
- **bit** (OPTIONAL): For the TCP protocol type only, enter one or a combination of the following TCP flags:
  - `ack` = acknowledgement
  - `fin` = finish (no more data from the user)
  - `psh` = push function
  - `rst` = reset the connection
  - `syn` = synchronize sequence number
  - `urg` = urgent field
- **operator** (OPTIONAL): For TCP and UDP parameters only. Enter one of the following logical operand:
  - `eq` = equal to
  - `neq` = not equal to
  - `gt` = greater than
  - `lt` = less than
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 | protocol-type [bit]} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator] command.

Parameters

- **redirect**: Enter the keyword redirect to assign the sequence to the redirect list.
- **ip-address**: Enter the IP address of the forwarding router.
- **slot/port**: Enter the keyword slot / port followed by the slot/port information.
- **tunnel**: Enter the keyword tunnel to configure the tunnel setting.
- **tunnel-id**: Enter the keyword tunnel-id to redirect the traffic.
- **track**: Enter the keyword track to enable the tracking.
track <obj-id>  
Enter the keyword track <obj-id> to track object-id.

ip-protocol-number  
Enter a number from 0 to 255 for the protocol identified in the IP protocol header.

protocol-type  
Enter one of the following keywords as the protocol type:
  - icmp for internet control message protocol
  - ip for any internet protocol
  - tcp for transmission control protocol
  - udp for user datagram protocol

bit  
(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags:
  - ack = acknowledgement
  - fin = finish (no more data from the user)
  - psh = push function
  - rst = reset the connection
  - syn = synchronize sequence number
  - urg = urgent field

source  
Enter the IP address of the network or host from which the packets were sent.

mask  
Enter a network mask in /prefix format (/x).

any  
Enter the keyword any to specify that all traffic is subject to the filter.

host ip-address  
Enter the keyword host then the IP address to specify a host IP address.

destination  
Enter the IP address of the network or host to which the packets are sent.

operator  
(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand:
  - eq = equal to
  - neq = not equal to
  - gt = greater than
  - lt = less than
  - range = inclusive range of ports (you must specify two ports for the port command parameter.)

Defaults  
None

Command Modes  
REDIRECT-LIST

Command History  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  
Description
9.8(1.0)  
Introduced on the Z9100-ON.
9.8(0.0P5)  
Introduced on the S4048-ON.
9.8(0.0P2)  
Introduced on the S3048-ON.
9.7(0.0)  
Introduced on the S6000-ON.
9.7(0.0)  
Added support for the track-id on the S4810, S4820T, S6000, and Z9000.
Version Description
9.5(0.1) Introduced on the Z9500.
9.4(0.0) Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1 Introduced on the C-Series and S-Series.
8.4.2.0 Introduced on the E-Series.
7.7.1.0 Introduced on the E-Series.

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

- `sequence-number`: Enter a number from 1 to 65535.
- `permit`: Enter the keyword permit assign the sequence to the permit list.
- `redirect`: Enter the keyword redirect to assign the sequence to the redirect list.
- `ip-address`: Enter the keyword IP address of the forwarding router.
- `tunnel`: Enter the keyword tunnel to configure the tunnel setting.
- `tunnel-id`: Enter the keyword tunnel-id to redirect the traffic.
- `track`: Enter the keyword track to enable the tracking.
- `track <obj-id>`: Enter the keyword track <obj-id> to track object-id.
- `ip-protocol-number`: Enter the keyword ip-protocol-number then the number from 0 to 255 for the protocol identified in the IP protocol header.
- `protocol-type`: Enter one of the following keywords as the protocol type:
  - `icmp` for internet control message protocol
  - `ip` for any internet protocol
  - `tcp` for transmission control protocol
  - `udp` for user datagram protocol
- `source`: Enter the IP address of the network or host from which the packets were sent.
- `mask`: Enter a network mask in /prefix format (/x).
- `any`: Enter the keyword any to specify that all traffic is subject to the filter.
- `host ip-address`: Enter the keyword host then the IP address to specify a host IP address.
**destination**

Enter the IP address of the network or host to which the packets are sent.

**bit**

(Optional) For the TCP protocol type only, enter one or a combination of the following TCP flags:

- **ack** = acknowledgement
- **fin** = finish (no more data from the user)
- **psh** = push function
- **rst** = reset the connection
- **syn** = synchronize sequence number
- **urg** = urgent field

**operator**

(Optional) For the TCP and UDP parameters only. Enter one of the following logical operand:

- **eq** = equal to
- **neq** = not equal to
- **gt** = greater than
- **lt** = less than
- **range** = inclusive range of ports (you must specify two ports for the port command parameter.)

**source port**

Enter the keywords `source-port` then the port number to be matched in the ACL rule in the ICAP rule.

**destination-port**

Enter the keywords `destination-port` then the port number to be matched in the ACL rule in the ICAP rule.

**source-port-range**

Enter the keywords `Source-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.

**destination-port-range**

Enter the keywords `destination-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.

**Defaults**

none

**Command Modes**

REDIRECT-LIST

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for the track-id on the S4810, S4820T, S6000, S6000-ON, and Z9000.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>
show cam pbr

Display the PBR CAM content.

Syntax

```
show cam pbr {interface interface | stack-unit slot-number port-set number [pipeline number]} [summary]
```

Parameters

- `interface interface`: Enter the keyword `interface` then the name of the interface.
- `stack-unit slot-number`: Enter the keyword `stack-unit` then the slot number.
- `port-set number`: Enter the keywords `port-set` then the port-pipe number.
- `summary`: Enter the keyword `summary` to view only the total number of CAM entries.

Defaults

none

Command Modes

EXEC

Command History

Version

- 9.8(1.0): Introduced on the Z9100-ON.
- 9.8(0.0P5): Introduced on the S4048-ON.
- 9.8(0.0P2): Introduced on the S3048-ON.
- 9.7(0.0): Introduced on the S6000-ON.
- 9.4(0.0): Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information

The `show cam pbr` command displays the PBR CAM content.

Example

```
Dell# show cam pbr stack-unit 1 port-set 0
TCP Flag: Bit 5 = URG, Bit 4 = ACK, Bit 3 = PSH, Bit 2 = RST,
Bit 1 = SYN, Bit 0 = FIN

Cam   Port VlanID Proto Tcp   Src   Dst   SrcIp          DstIp         Next-hop        Egress
Index                   Flag  Port  Port                               MAC               Port
----------------------------------------------------------------------------------
00000 5 N/A   IP   0x0   0     0     22.22.22.22/32  33.33.33.0/24  00:01:e8:8a:fd:76 0/0
00001 5 N/A   TCP  0x0   0     0     0.0.0.0/0      44.4.4.4/32   00:01:e8:8a:fd:76 Vl 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 ip redirect-list

View the redirect list configuration and the interfaces it is applied to.

Syntax

```
show ip redirect-list redirect-list-name
```

Parameters

- `redirect-list-name` Enter the name of a configured Redirect list.

Command Modes

- EXEC
- EXEC Privilege

Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>

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 Gi 1/32)
  seq 10 redirect tunnel 1 track 1 tcp any any, Track 1 [up],
  Next-hop reachable (via Gi 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 Gi 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 Gi 1/32)
  , 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 Gi 2/18)
  , Track 200 [up], Next-hop reachable (via Gi 2/19)
Dell#
```
PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast (PIM) commands are supported by the Dell Networking operating software on the platform. The following describes the IPv4 PIM-SIM commands.

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

clear ip pim rp-mapping

The bootstrap router (BSR) feature uses this command to remove all or particular rendezvous point (RP) advertisement.

Syntax

```
clear ip pim [vrf vrf-name] rp-mapping [rp-address]
```

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.

  > **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- `rp-address` (OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
This command re-applies the RP mapping logic for all the groups learnt by the node. Any stale information corresponding to the existing mapping configuration is updated. The existing BSR cache and the *.G's are deleted only if these entries are stale.

**clear ip pim tib**

Clear PIM tree information from the PIM database.

**Syntax**

`clear ip pim [vrf vrf-name] tib [group]`

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.
  
  **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- `group` (OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**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.

default ip pim {vrf vrf-name} {bsr | events | group | packet [in | out] | register | state | timer [assert | hello | joinprune | register]}

To disable PIM debugging, use the no debug ip pim {vrf vrf-name} command or use the undebug
all to disable all debugging command.

Parameters

vrf vrf-name
(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to view IP PIM
debugging messages corresponding to that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default
VRF.

bsr
(OPTIONAL) Enter the keyword bsr to view PIM Candidate RP/BSR activities.

events
(OPTIONAL) Enter the keyword group to view PIM messages for a specific group.

group
(OPTIONAL) Enter the keyword group to view PIM messages for a specific group.

packet [in | out]
(OPTIONAL) Enter the keyword packet to view PIM packets. Enter one of the optional
parameters:

• in: to view incoming packets
• out: to view outgoing packets

register
(OPTIONAL) Enter the keyword register to view PIM register address in dotted
decimal format (A.B.C.D).

state
(OPTIONAL) Enter the keyword state to view PIM state changes.

timer [assert | hello | joinprune | register]
(OPTIONAL) Enter the keyword timer to view PIM timers. Enter one of the optional
parameters:

• assert: to view the assertion timer
• hello: to view the PIM neighbor keepalive timer
• joinprune: to view the expiry timer (join/prune timer)
• register: to view the register suppression timer

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P6) Introduced on the S4048-ON.
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

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 [vrf vrf-name] bsr-candidate interface [hash-mask-length] [priority]

To return to the default value, use the no ip pim bsr-candidate [vrf vrf-name] command.

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure the PIM router on a VRF.

interface    Enter the following keywords and slot/port or number information:

  • For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  • For a Port Channel interface, enter the keywords_port-channel then a number.
  • For a VLAN, enter the keyword vlan then a number from 1 to 4094.
  • For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  • For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

hash-mask-length  (OPTIONAL) Enter the hash mask length. The range is from zero (0) to 32. The default is 30.

priority  (OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is zero (0).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version   Description
9.8(1.0)   Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.5(0.1)   Introduced on the Z9500.
9.0.2.0     Introduced on the S6000.
8.3.19.0    Introduced on the S4820T.
8.3.11.1    Introduced on the Z9000.
8.3.7.0     Introduced on the S4810.
8.11.0      Introduced on the E-Series.
6.1.1.0     Added support for the VLAN interface.
**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**

`priority-value` Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.

**Defaults**

1

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series on port-channels and the S-Series.</td>
</tr>
</tbody>
</table>

**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 [vrf vrf-name] join-filter ext-access-list [in | out]
```

To remove the access list, use the `no ip pim [vrf vrf-name] join-filter ext-access-list` command.
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to permit or deny PIM join or prune messages on an interface associated with that VRF.</td>
</tr>
<tr>
<td>ext-access-list</td>
<td>Enter the name of an extended access list.</td>
</tr>
<tr>
<td>in</td>
<td>Enter the keyword in to apply the ACL filter to in-bound traffic.</td>
</tr>
<tr>
<td>out</td>
<td>Enter the keyword out to apply the ACL filter to out-bound traffic.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Removed the in and out parameters. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series for the port-channels and the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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-ext-nacl)#

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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>std-access-list</td>
<td>Enter the name of a standard access list.</td>
</tr>
</tbody>
</table>

**Defaults**
none
**ip pim neighbor-filter**

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

**Syntax**

```
ip pim [vrf vrf-name] neighbor-filter {access-list}
```

To remove the restriction, use the
```
no ip pim [vrf vrf-name] neighbor-filter {access-list}
```

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to prevent that VRF from participating in PIM.

  **NOTE:** Applies to specific VRF if input is provided, else applies to default VRF.

- **access-list** Enter the name of a standard access list. Maximum 16 characters.

**Defaults**

- none

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command restricts a particular neighbor from receiving PIM packets. Neighbor-filtering is supported for PIM neighbors discovered using Rendezvous Point (RP) and Bootstrap Router (BS) discovery.

When applied, this configuration filters received PIM join and prune messages from the specified neighbor. This configuration does not filter PIM hello messages.
Usage Information
Do not enter this command before creating the access-list.

**ip pim query-interval**

Change the frequency of PIM Router-Query messages.

**Syntax**
```
ip pim query-interval seconds
```
To return to the default value, use the `no ip pim query-interval seconds` command.

**Parameters**
- **seconds**
  Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is 30 seconds.

**Defaults**
30 seconds

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.1.1.0 | Introduced on the E-Series.
7.8.1.0 | Introduced on the C-Series and S-Series.
7.6.1.0 | Introduced on the E-Series.
**ip pim register-filter**

To prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group, use this feature.

**Syntax**

```
ip pim [vrf vrf-name] register-filter access-list
```

To return to the default, use the `no ip pim [vrf vrf-name] register-filter access-list` command.

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF.

  **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- **access-list** Enter the name of an extended access list. Maximum 16 characters.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list.
ip pim rp-address

Configure a static PIM rendezvous point (RP) address for a group or access-list.

Syntax

ip pim [vrf vrf-name] rp-address address {group-address group-address mask} [override]

To remove an RP address, use the no ip pim [vrf vrf-name] rp-address address {group-address group-address mask} [override] command.

Parameters

vrf vrf-name

(Optional) Enter the keyword vrf followed by the name of the VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

address

Enter the RP address in dotted decimal format (A.B.C.D).

group-address

group-address

Enter the keywords group-address then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.

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

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(10) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.5(0.1) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

8.1.1.0 Introduced on the E-Series.

7.8.1.0 Introduced on the S-Series.

pre- 6.1.1.1 Introduced on the E-Series.
Usage Information

First-hop routers use this address by to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. The RP is chosen based on a longer prefix match for a group. The RP selection does not depend on dynamic or static RP assignments.

ip pim rp-candidate

To send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR, configure a PIM router.

Syntax

```
ip pim [vrf vrf-name] rp-candidate {interface [priority]}
```

To return to the default value, use the `no ip pim [vrf vrf-name] rp-candidate {interface [priority]}` command.

Parameters

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF.

  NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

- `interface` Enter the following keywords and slot/port or number information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
  - For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

- `priority` (OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is 192.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Added support for VRF. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
Version Description
pre-6.1.1.1 Introduced on the E-Series.

Usage Information Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

**ip pim sparse-mode**

Enable PIM sparse mode and IGMP on the interface.

**Syntax**

```
ip pim sparse-mode
```

To disable PIM sparse mode and IGMP, use the

```
no ip pim sparse-mode
```

**Defaults**

Disabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series for the port-channels and the S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The interface must be enabled (the no shutdown command) and not have the switchport command configured. Multicast must also be enabled globally (using the ip multicast-lag-hashing command). PIM is supported on the port-channel interface.

**ip pim sparse-mode sg-expiry-timer**

Enable expiry timers globally for all sources.

**Syntax**

```
ip pim [vrf vrf-name] sparse-mode sg-expiry-timer seconds [access-list-name]
```

PIM-Sparse Mode (PIM-SM) | 1129
To disable configured timers and return to default mode, use the `no ip pim [vrf vrf-name] sparse-mode sg-expiry-timer` command.

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable expiry timer for all sources on that VRF.

  **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.

- `seconds` Enter the number of seconds the S, G entries are retained. The range is from 211 to 65535.

- `access-list-name` (OPTIONAL) Enter the name of a previously configured Extended ACL to enable the expiry time to specified S,G entries.

**Defaults**

Disabled. The default expiry timer (with no times configured) is 210 sec.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series for the port-channels and the S-Series.</td>
</tr>
<tr>
<td>7.7.1.1</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL. Even though the FHR nodes act as RPs, these nodes still send Register encap messages to themselves and expect to receive a Register stop message (for Anycast RP support). As a result, if the DLT timer expires, SG is not deleted until the register state is deleted in the node. This register state expires 210 seconds after the last Null register is received.

**ip pim ssm-range**

Specify the SSM group range using an access list.

**Syntax**

`ip pim [vrf vrf-name] ssm-range {access_list_name}`

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to specify the SSM group range for that VRF.
NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

```
access_list_name
```
Enter the name of the access list.

**Defaults**
Default SSM range is 232/8 and ff3x/32

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON. Added support for VRF on S6000, S4810, S4820T, Z9000, Z9500, and S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
Dell Networking OS supports standard access lists for the SSM range. You cannot use extended ACLs for configuring the SSM range. If you configure an extended ACL and then used in the `ip pim ssm-range {access list name}` configuration, an error is reported.

However, if you configure `ip pim ssm-range {access list name}` first and then you configure the ACL as an Extended ACL, an error is not reported and the ACL is not applied to the SSM range.

Dell Networking OS-recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. After the SSM range is applied, the changes are applied internally without requiring clearing of the tree information base (TIB).

When the ACL rules change, the ACL and protocol-independent multicast (PIM) modules apply the new rules automatically.

When you configure the SSM range, Dell Networking OS supports SSM for configured group range as well as the default SSM range.

When you remove the SSM ACL, PIM SSM is supported for the default SSM range only.
ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

Syntax

```
ip pim [vrf vrf-name] spt-threshold [value | infinity]
```

To return to the default value, use the `no ip pim [vrf vrf-name] spt-threshold [infinity]` command.

Parameters

- **value** (OPTIONAL) Enter the traffic value in kilobits per second. The default is 10 packets per second. A value of zero (0) causes a switchover on the first packet.
- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure the PIM router on that VRF.
  
  **NOTE:** Applies to specific VRF if input is provided, else applies to Default VRF.
- **infinity** (OPTIONAL) Enter the keyword `infinity` to never switch to the source-tree.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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.

Syntax

```
no ip pim snooping dr-flood
```

To re-enable the flooding of multicast packets to the PIM designated router, use the `ip pim snooping dr-flood` command.
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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

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 designated-router flooding.

When designated-router flooding 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.

If the PIM DR flood is not disabled (default setting):

- Multicast traffic is transmitted on the egress port towards the PIM DR if the port is not the incoming interface.
- 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.

show ip pim bsr-router

View information on the Bootstrap router.

S3048-ON

Syntax

show ip pim [vrf vrf-name] bsr-router

Parameters

vrf vrf-name

(Optional) Enter the keyword vrf followed by the name of the VRF to configure this setting on VRF.

Note: Applies to specific VRF if input is provided, else applies to Default VRF.

Command Modes

- EXEC
- EXEC Privilege
**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Example**

Dell# show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask length: 30
Dell#

**show ip pim interface**

View information on the interfaces with IP PIM enabled.

**S3048-ON**

**Syntax**

```
show ip pim [vrf vrf-name] interface
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on this VRF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*. 
### Usage Information

The following describes the `show ip pim interface` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Lists the IP addresses of the interfaces participating in PIM.</td>
</tr>
<tr>
<td>Interface</td>
<td>Lists the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.</td>
</tr>
<tr>
<td>Ver/Mode</td>
<td>Displays the PIM version number and mode for each interface participating in PIM:</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Displays the number of PIM neighbors discovered over this interface.</td>
</tr>
<tr>
<td>Query Intvl</td>
<td>Displays the query interval for Router Query messages on that interface (configured with <code>ip pim query-interval</code> command).</td>
</tr>
<tr>
<td>DR Prio</td>
<td>Displays the Designated Router priority value configured on the interface (use the <code>ip pim dr-priority</code> command).</td>
</tr>
<tr>
<td>DR</td>
<td>Displays the IP address of the Designated Router for that interface.</td>
</tr>
</tbody>
</table>

The `show ip pim interface` command does not display information corresponding to the loop-back interfaces.

### Example

```
Dell# show ip pim interface
Address          Interface  Ver/Mode  Nbr Count  Query Intvl  DR Prio  DR
165.87.34.5      Gi 1/10    v2/S      0         30           1       165.87.34.5
10.1.1.2         Vl 10      v2/S      1         30           1       10.1.1.2
20.1.1.5         Vl 20      v2/S      1         30           1       20.1.1.5
165.87.31.200    Vl 30      v2/S      1         30           1       165.87.31.201
```

Dell#
**show ip pim neighbor**

View PIM neighbors.

**S3048–ON**

**Syntax**

```
show ip pim [vrf vrf-name] neighbor
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show ip pim neighbor` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor address</td>
<td>Displays the IP address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.</td>
</tr>
<tr>
<td>Uptime/expires</td>
<td>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).</td>
</tr>
<tr>
<td>Ver</td>
<td>Displays the PIM version number.</td>
</tr>
</tbody>
</table>

- `v2 = PIM version 2`
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR prio/Mode</td>
<td>Displays the Designated Router priority and the mode.</td>
</tr>
<tr>
<td></td>
<td>• 1 = default Designated Router priority (use the <code>ip pim dr-priority</code> command)</td>
</tr>
<tr>
<td></td>
<td>• DR = Designated Router</td>
</tr>
<tr>
<td></td>
<td>• S = Sparse mode</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show ip pim neighbor
Neighbor  Interface  Uptime/Expires  Ver DR
Address                                       Prio/Mode
127.87.3.4 Gi 1/16  09:44:58/00:01:24  v2  1 / S
Dell#
```

### show ip pim rp

View all multicast groups-to-RP mappings.

**S3048-ON**

**Syntax**

```
show ip pim [vrf vrf-name] rp [mapping | group-address]
```

**Parameters**

- **vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.
- **mapping** (OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
- **group-address** (OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.5(0.1) Introduced on the Z9500.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.12.0 Introduced on the S4810.
- 8.4.1.1 Introduced on the E-Series.

**Usage Information**

The following describes the `show ip pim snooping interface` commands shown in the following example.

```
Example   Dell# show ip pim rp
          Group    RP
          224.2.197.115  165.87.20.4
          224.2.217.146  165.87.20.4
          224.3.3.3      165.87.20.4
          225.1.2.1      165.87.20.4
          225.1.2.2      165.87.20.4
          229.1.2.1      165.87.20.4
          229.1.2.2      165.87.20.4
          Dell#

Example (Mapping) Dell# show ip pim rp mapping
                PIM Group-to-RP Mappings
                Group(s): 224.0.0.0/4, Static
                RP: 50.40.4.4, v2
                Dell#

Example (Address) Dell# show ip pim rp 229.1.2.1
                   Group    RP
                   229.1.2.1  165.87.20.4
                   Dell#
```
### show ip pim snooping interface

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

#### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

#### Usage Information

The following describes the `show ip pim snooping neighbor` commands shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor address</td>
<td>Displays the IP address of the neighbor learned through PIM-SM snooping.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
**Interface** | Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
**Uptime/expires** | Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
**Ver** | Displays the PIM version number:
- $v2$ = PIM version 2
**DR prio/Mode** | Displays the Designated Router priority and the mode:
- $1$ = default Designated Router priority (use the `ip pim dr-priority` command)
- $DR$ = Designated Router
- $S$ = Sparse mode

**Example**

```
Dell# show ip pim snooping neighbor
Neighbor  Interface          Uptime/Expires    Ver  DR Prio
Address
165.87.32.2 Vl 2 [Gi 1/13 ]  00:04:03/00:01:42  v2  1
165.87.32.10 Vl 2 [Gi 1/11 ]  00:00:46/00:01:29  v2  0
165.87.32.12 Vl 2 [Gi 2/20 ] 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.5(0.1) | Introduced on the Z9500.
8.3.19.0 | Introduced on the S4820T.
### Version and Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

The following describes the `show ip pim snooping tib` commands shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the PIM multicast snooping database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM multicast route table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
<tr>
<td>flags</td>
<td>List the flags to define the entries:</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse Mode</td>
</tr>
<tr>
<td></td>
<td>• C = directly connected</td>
</tr>
<tr>
<td></td>
<td>• L = local to the multicast group</td>
</tr>
<tr>
<td></td>
<td>• P = route was pruned</td>
</tr>
<tr>
<td></td>
<td>• R = the forwarding entry is pointing toward the RP</td>
</tr>
<tr>
<td></td>
<td>• F = Dell Networking OS is registering this entry for a multicast source</td>
</tr>
<tr>
<td></td>
<td>• T = packets were received via Shortest Tree Path</td>
</tr>
<tr>
<td></td>
<td>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</td>
</tr>
<tr>
<td></td>
<td>• K=acknowledge pending state</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) interface towards the RP/source.</td>
</tr>
<tr>
<td>RPF neighbor</td>
<td>Displays the next hop from this interface towards the RP/source.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Lists the interfaces that meet one of the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• a directly connect member of the Group</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) Join message</td>
</tr>
</tbody>
</table>

### 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:
  GigabitEthernet 2/11 RPF 165.87.32.2 00:00:01/00:02:59
  GigabitEthernet 2/13 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
```
show ip pim ssm-range

Display the non-default groups added using the SSM range feature.

3048–ON

Syntax

show ip pim [vrf vrf-name] ssm-range

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON. Added support for VRF on S6000, S4810, S4820T, Z9000, Z9500, and S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Example

Group Address / MaskLen
show ip pim summary

View information about PIM-SM operation.

S3048-ON

Syntax

show ip pim [vrf vrf-name] summary

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(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.
9.5(0.1) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.4.1.1 Support for the display of PIM-SM snooping status was added on E-Series.
8.1.1.0 Introduced on the E-Series.
7.8.1.0 Introduced on the S-Series.

Example

Dell# show ip pim summary
PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2

Active Modes :
PIM-SNOOPING

Interface summary:
  1 active PIM interface
  0 passive PIM interfaces
  3 active PIM neighbors

TIB summary:
  1/1 (*,G) entries in PIM-TIB/MFC
  1/1 (S,G) entries in PIM-TIB/MFC
show ip pim tib

View the PIM tree information base (TIB).

S3048-ON

Syntax

show ip pim [vrf vrf-name] tib [group-address [source-address]]

Parameters

vrf vrf-name  (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

group-address  (OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).

source-address  (OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

-  EXEC
-  EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0)  Introduced on the Z9100-ON.

9.8(0.0P5)  Introduced on the S4048-ON.

9.8(0.0P2)  Introduced on the S3048-ON.

9.5(0.1)  Introduced on the Z9500.

9.0.2.0  Introduced on the S6000.
The following describes the `show ip pim tib` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S, G)</td>
<td>Displays the entry in the multicast PIM database.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the amount of time the entry has been in the PIM route table.</td>
</tr>
<tr>
<td>expires</td>
<td>Displays the amount of time until the entry expires and is removed from the database.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays the IP address of the RP/source for this entry.</td>
</tr>
<tr>
<td>flags</td>
<td>List the flags to define the entries:</td>
</tr>
<tr>
<td></td>
<td>• D = PIM Dense Mode</td>
</tr>
<tr>
<td></td>
<td>• S = PIM Sparse Mode</td>
</tr>
<tr>
<td></td>
<td>• C = directly connected</td>
</tr>
<tr>
<td></td>
<td>• L = local to the multicast group</td>
</tr>
<tr>
<td></td>
<td>• P = route was pruned</td>
</tr>
<tr>
<td></td>
<td>• R = the forwarding entry is pointing toward the RP</td>
</tr>
<tr>
<td></td>
<td>• F = Dell Networking OS is registering this entry for a multicast source</td>
</tr>
<tr>
<td></td>
<td>• T = packets were received via Shortest Tree Path</td>
</tr>
<tr>
<td></td>
<td>• J = first packet from the last hop router is received and the entry is ready to switch to SPT</td>
</tr>
<tr>
<td></td>
<td>• K = acknowledge pending state</td>
</tr>
<tr>
<td>Incoming interface</td>
<td>Displays the reverse path forwarding (RPF) interface towards the RP/source.</td>
</tr>
<tr>
<td>RPF neighbor</td>
<td>Displays the next hop from this interface towards the RP/source.</td>
</tr>
<tr>
<td>Outgoing interface list</td>
<td>Lists the interfaces that meet one of the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• a directly connect member of the Group</td>
</tr>
<tr>
<td></td>
<td>• statically configured member of the Group</td>
</tr>
<tr>
<td></td>
<td>• received a (*,G) Join message</td>
</tr>
</tbody>
</table>

Example

Dell# do show ip pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned, 
R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, 
M - MSDP created entry, A - Candidate for MSDP Advertisement 
K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:40:16, expires 00:00:00, RP 20.40.4.4, flags: SCJ 
Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4 
Outgoing interface list: 
Vlan 2006  Forward/Sparse   00:06:21/Never
show running-config pim

Display the current configuration of PIM-SM snooping.

Syntax
show running-config pim

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.
8.4.1.0 Introduced on the E-Series.

Example
Dell# show running-config pim
!
ip pim snooping enable
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 and logical interfaces, such as port channels and virtual local area networks (VLANs).
- The monitoring (destination, “MG”) and monitored (source, “MD”) ports must be on the same switch.
- In general, a monitoring port should have no ip address and no shutdown as the only configuration; Dell Networking OS permits a limited set of commands for monitoring ports; display them using the ? command. A monitoring port also may not be a member of a VLAN.
- A total of 4 MG may be configured in a single port-pipe.
- MG and MD ports can be reside anywhere across a port-pipe.
- The Dell Networking OS supports multiple source ports to be monitored by a single destination port in one monitor session.
- One monitor session can have only one MG port.

**NOTE:** The monitoring port should not be a part of any other configuration.

Topics:
- description
- monitor multicast-queue
- monitor session
- rate-limit
- 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**
- CONFIGURATION
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Related Commands

- `monitor session` — enables a monitoring session.

## monitor multicast-queue

Configure monitor QoS multicast queue ID.

**Syntax**

```
monitor multicast-queue queue-id
```

To remove the configuration, use the `no monitor multicast-queue` command.

**Parameters**

- `queue-id`  
  Enter the QoS multicast queue ID. The range is from 0 to 9.

**Defaults**

```
queue-id: 0
```

Enable status: Disabled

**Command Modes**

CONFIGURATION

**Example**

```
Dell(conf)#monitor multicast-queue 7
```

**Command History**

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.
**monitor session**

Create a session for monitoring traffic with port monitoring.

**Syntax**

```
monitor session session-ID [type { rpm | erpm [set ip dscp dscp_value | set ip ttl ttl_value]]} [drop]
```

To delete a session, use the `no monitor session session-ID` command.

To delete all monitor sessions, use the `no monitor session all` command.

**Parameters**

- `session-ID` Enter a session identification number. The range is from 0 to 65535.
- `type` Specifies one of the following type:
  - `rpm`
  - `erpm`
- `rpm` Creates a remote port monitoring (rpm) session.
- `erpm` Creates an encapsulated remote port monitoring (erpm) session.
- `set ip dscp` Configures the Differentiated Services Code Point (DSCP) value of the packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic. To revert to the default value, use the `no form of this command`.
  - `dscp_value` DSCP value of the packets in the ERSPAN traffic. The range is from 0 to 63. The default value is 0.
- `set ip ttl` Configures the IP time-to-live (TTL) value of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic. To revert to the default configuration, use the `no form of this command`.
  - `ttl_value` IP TTL value of the ERSPAN traffic. The range is from 1 to 255. The default value is 255.
- `drop` Monitors only the dropped packets in the Ingress.

**Defaults**

- `none`

**Command Modes**

- `CONFIGURATION`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
### Version Description

- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.8(0.0)** Added the drop parameter.
- **9.7(0.0)** Introduced on the S6000-ON. Introduced the `set ip dscp` and `set ip ttl` parameters.
- **9.5(0.1)** Introduced on the Z9500.
- **9.4(0.0)** Introduced on the S4810, S4820T, S6000, and Z9000.
- **9.0.2.0** Introduced on the S6000.
- **9.0.2.0** Introduced on the MXL.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.7.0** Introduced on the S4810.

### Usage Information

The `monitor` command is saved in the running configuration at Monitor Session mode level and can be restored after a chassis reload.

### Example

```
Dell# show monitor session
SessID  Source         Destination         Dir  Mode  Source IP      Dest IP         DSCP  TTL
------  ------         -----------         ---  ----  ---------      --------        ----  ---
0   Gi 1/12           remote-ip         rx   Flow 1.1.1.1         7.1.1.2         0     255
0   Po 1              remote-ip         tx   Flow 1.1.1.1         7.1.1.2         0     255
1   Vl 11             remote-ip         rx   Flow 5.1.1.1         3.1.1.2         0     255
```

### Related Command

- `show monitor session` — displays the monitor session.
- `show running-config monitor session` — displays the running configuration of a monitor session.

## rate-limit

Configure the rate-limit to limit the mirrored packets.

### Syntax

```
rate-limit limit
```

To remove the limit, use the `no rate-limit limit` command.

### Parameters

- **limit**
  
  Enter the rate-limit value. The range is from 0 to 40000 Megabits per second.

### Defaults

- **60**

### Command Modes

- **CONFIGURATION**

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

- **9.8(1.0)** Introduced on the Z9100-ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.8(0.0)** Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9500.
Related Commands

- `monitor session` — enable a monitoring session.
- `show monitor session` — display the monitor session.

**show config**

Display the current monitor session configuration.

**Syntax**

```
show config
```

**Defaults**

```
none
```

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

Dell(conf-mon-sess-1)# show config

```
monitor session 1
  source GigabitEthernet 1/1 destination Port-channel 1 direction rx
```

**show monitor session**

Display information about monitoring 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.
show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

Syntax

```
show running-config monitor session {session-ID}
```

To display the running configuration for all monitor sessions, use the `show running-config monitor session` command.
**Parameters**

- **session-ID** (OPTIONAL) Enter a session identification number. The range from 0 to 65535.

**Defaults**

- none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `monitoring` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

**Example**

```
Dell# show running-config monitor session
!
monitor session 1
source GigabitEthernet 1/1 destination GigabitEthernet 1/2 direction rx
!
monitor multicast-queue 7
Dell#
```

**Related Commands**

- `monitor session` — creates a monitoring session.
- `show monitor session` — displays a monitoring session.

---

**source (port monitoring)**

Configure a port monitor source.

**Syntax**

```
source {interface | range | any} destination interface direction {rx | tx | both}
```
To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

**Parameters**

<table>
<thead>
<tr>
<th>field</th>
<th>description</th>
</tr>
</thead>
</table>
| source interface | Enter one of the following keywords and slot/port information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `VLAN` followed by a number from 1 to 4094.
  - For a port channel interface, enter the keywords `port-channel` then a number. |
| range | Enter the keyword `range` to specify the list of interfaces. |
| any | Enter the keyword `any` to specify all interfaces. |
| NOTE: This option is applicable only with drop monitor session. |
| destination | Enter the keyword `destination` to specify the destination interface.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number. |
| interface | Enter one of the following keywords and slot/port information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `Vlan` then a number from 1 to 4094.
  - For a port channel interface, enter the keywords `port-channel` then a number. |
| direction (rx | tx | both) | Enter the keyword `direction` then one of the packet directional indicators.
  - `rx`: to monitor receiving packets only.
  - `tx`: to monitor transmitting packets only.
  - `both`: to monitor both transmitting and receiving packets. |

**Defaults**

none

**Command Modes**

MONITOR SESSION (conf-mon-sess-session-ID)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the <code>any</code> parameter.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4.0.0</td>
<td>Added support for Source and destination.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

Dell# monitor session 0
source Port-channel 10 destination GigabitEthernet 1/3 direction tx
Dell#
Private VLAN (PVLAN)

The private VLAN (PVLAN) feature of the Dell Networking OS is supported on the platforms. Private VLANs extend the Dell Networking OS security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair. The Dell Networking OS private VLAN implementation is based on RFC 3069.

For more information, see the following commands. The command output is augmented in Dell Networking OS version 7.8.1.0 at later to provide PVLAN data:

- show arp
- show vlan

Private VLAN Concepts

Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice versa.

Port Types:

- Community port — a community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- Isolated port — an isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- Promiscuous port — a promiscuous port is a port that is allowed to communicate with any other port type.
- Trunk port — a trunk port carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - A trunk port in Tagged mode carries primary or secondary VLAN traffic. The tag on the packet helps identify the VLAN to which the packet belongs.
  - A trunk port can also belong to a regular VLAN (non-private VLAN).
ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

S3048

Syntax

[no] ip local-proxy-arp

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the no ip local-proxy-arp command in INTERFACE VLAN mode for the primary VLAN.

To disable Layer 3 communication in a particular secondary VLAN, use the no ip local-proxy-arp command in INTERFACE VLAN mode for the selected secondary VLAN.

**NOTE:** Even after you disable ip-local-proxy-arp (use no ip-local-proxy-arp) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the address resolution protocol (ARP) timeout happens on those secondary VLAN hosts.

Defaults

Layer 3 communication is disabled between secondary VLANs in a private VLAN.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

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.
private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

**S3048**

**Syntax**

```
[no] private-vlan mode {community | isolated | primary}
```

To remove the PVLAN configuration, use the `no private-vlan mode {community | isolated | primary}` command syntax.

**Parameters**

- **community**
  - Enter the keyword `community` to set the VLAN as a community VLAN.
- **isolated**
  - Enter the keyword `isolated` to configure the VLAN as an isolated VLAN.
- **primary**
  - Enter the keyword `primary` to configure the VLAN as a primary VLAN.

**Defaults**

none

**Command Modes**

INTERFACE VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The VLAN:

- can be in only one mode, either community, isolated, or primary.
- mode to community or isolated even before associating it to a primary VLAN. This secondary VLAN continues to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message indicates this.)
- must not have a port in it when VLAN mode is being set.

Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as previously described) can be added to the PVLAN. No other regular ports can be added to the PVLAN.
After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

**Related Commands**
- `private-vlan mapping secondary-vlan` — maps secondary VLANs to the selected primary VLAN.
- `switchport mode private-vlan` — sets PVLAN mode of the selected port.

### private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

**S3048**

**Syntax**

```
[no] private-vlan mapping secondary-vlan vlan-list
```

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` command syntax.

**Parameters**

- **vlan-list**
  
Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.

**Defaults**

none

**Command Modes**

INTERFACE VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the C-Series and S-Series.

**Usage Information**

The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.
- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.
Related Commands

- private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.
- switchport mode private-vlan — sets PVLAN mode of the selected port.

switchport mode private-vlan

Set PVLAN mode of the selected port.

S3048

Syntax

[no] switchport mode private-vlan {host | promiscuous | trunk}

To remove PVLAN mode from the selected port, use the no switchport mode private-vlan command.

Parameters

- **host**: Enter the keyword host to configure the selected port or port channel as an isolated interface in a PVLAN.
- **promiscuous**: Enter the keyword promiscuous to configure the selected port or port channel as a promiscuous interface.
- **trunk**: Enter the keyword trunk to configure the selected port or port channel as a trunk port in a PVLAN.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.1(0.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

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-gi-2/1)# switchport mode private-vlan promiscuous
```
Dell(conf)# interface GigabitEthernet 2/2
Dell(conf-if-gi-2/2)# switchport mode private-vlan host

Dell(conf)# interface GigabitEthernet 2/3
Dell(conf-if-gi-2/3)# switchport mode private-vlan trunk

Dell(conf)# interface port-channel 10
Dell(conf-if-gi-2/3)# switchport mode private-vlan promiscuous
Dell(conf-if-gi-2/3)#

Related Commands

- **private-vlan mode** — sets the mode of the selected VLAN to community, isolated, or primary.
- **private-vlan mapping secondary-vlan** — sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it.
Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking OS implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1w standard spanning tree protocol.

Dell Networking OS supports PVST+ on the S3048 platform.

**NOTE:** For easier command line entry, the plus (+) sign is not used at the command line.

Topics:
- description
- disable
- extend system-id
- protocol spanning-tree pvst
- show spanning-tree pvst
- spanning-tree pvst
- spanning-tree pvst err-disable
- tc-flush-standard
- vlan bridge-priority
- vlan forward-delay
- vlan hello-time
- vlan max-age

### description

Enter a description of the PVST+.

**S3048**

**Syntax**

```
description {description}
```

To remove the description, use the `no description {description}` command.

**Parameters**

- `description` Enter a description to identify the spanning tree (80 characters maximum).

**Defaults**

- none

**Command Modes**

SPANNING TREE PVST+ (The prompt is “config-pvst”)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
**disable**

Disable PVST+ globally.

**S3048**

**Syntax**

```plaintext
disable
```

To enable PVST+, use the `no disable` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION (conf-pvst)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>pre-7.7.1.1</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `protocol spanning-tree pvst` — enter SPANNING TREE mode on the switch.
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.

S3048

Syntax
extend system-id

Defaults
Disabled

Command Modes
PROTOCOL PVST

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.3.1.0 Introduced.

Example
Dell(conf-pvst)# do show spanning-tree pvst vlan 5 brief
VLAN 5
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32773, Address 0001.e832.73f7
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32773 (priority 32768 sys-id-ext 5), Address 0001.e832.73f7
We are the root of Vlan 5
Configured hello time 2, max age 20, forward delay 15

Interface Designated
Name    PortID  Prio  Cost  Sts Cost Bridge ID      PortID
-------------------------------------------------------------
Gi 1/10 128.140 128  200000 FWD 0   32773 0001.e832.73f7 128.140
Gi 1/12 128.142 128  200000 DIS 0   32773 0001.e832.73f7 128.142

Interface
Name    Role PortID  Prio  Cost Sts Cost Link-type Edge
-------- ------- ------ ------ ------ -------------  -------------

protocol spanning-tree pvst

To enable PVST+ on a device, enter the PVST+ mode.

S3048

Syntax

protocol spanning-tree pvst

To disable PVST+, use the disable command.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

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

Related Commands

- protocol spanning-tree pvst – enter SPANNING TREE mode on the switch.
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 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Port Channel interface, enter the keyword port-channel then a number.
- **guard** (OPTIONAL) Enter the keyword guard to display the type of guard enabled on a PVST interface and the current port state.

Defaults

- none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
**Usage Information**

The following describes the `show spanning-tree pvst` command shown in the following examples.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Name</strong></td>
<td>PVST interface.</td>
</tr>
<tr>
<td><strong>Instance</strong></td>
<td>PVST instance.</td>
</tr>
<tr>
<td><strong>Sts</strong></td>
<td>Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).</td>
</tr>
<tr>
<td><strong>Guard Type</strong></td>
<td>Type of STP guard configured (Root, Loop, or BPDU guard).</td>
</tr>
</tbody>
</table>

**Example (Brief)**

```
Dell# show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4096, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface Name PortID Prio Cost Sts Cost Bridge ID PortID
----------------------------------------------------------
Gi 1/0 128.130 128 20000 FWD 20000 4096 0001.e801.6aa8 128.426
Gi 1/1 128.131 128 20000 BLK 20000 4096 0001.e801.6aa8 128.427
Gi 1/16 128.146 128 20000 FWD 20000 16384 0001.e805.e306 128.146
Gi 1/17 128.147 128 20000 FWD 20000 16384 0001.e805.e306 128.147

Interface Name Role PortID Prio Cost Sts Cost Link-type Edge
--------------------------------------------------------------
Gi 1/0 Root 128.130 128 20000 FWD 20000 P2P No
Gi 1/1 Altr 128.131 128 20000 BLK 20000 P2P No
Gi 1/16 Desg 128.146 128 20000 FWD 20000 P2P Yes
Gi 1/17 Desg 128.147 128 20000 FWD 20000 P2P Yes
```

**Example**

```
Dell# show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
Number of topology changes 3, last change occured 00:57:00

Port 130 (GigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.130
```
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (GigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1576, received 0
The port is not in the Edge port mode

Port 146 (GigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode

Port 147 (GigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode

Example (EDS/LBK)
Dell# show spanning-tree pvst vlan 2 interface gigabitethernet 1/1

GigabitEthernet 1/1 of VLAN 2 is LBK_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

Interface Designated
Name    PortID   Prio Cost  Sts Cost Bridge ID       PortID
-----------------------------------------------------------
Gi 1/1 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223

Example (EDS/PVID)
Dell# show spanning-tree pvst vlan 2 interface gigabitethernet 1/1

GigabitEthernet 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
-----------------------------------------------------------
Gi 1/1 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223

Example (Guard)
Dell# show spanning-tree pvst vlan 5 guard

Interface
Name     Instance Sts Guard type
-----------------------------------
Gi 1/1   5       INCON(Root) Rootguard
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]] | err-disable | vlan vlan-range {cost number | priority value} | loopguard | rootguard}

Parameters

- **edge-port**
  - Enter the keywords edge-port to configure the interface as a PVST+ edge port.

- **bpduguard**
  - Enter the keyword portfast to enable Portfast to move the interface into Forwarding mode immediately after the root fails.
  - Enter the keyword bpduguard to disable the port when it receives a BPDU.

- **shutdown-on-violation** (OPTIONAL)
  - Enter the keywords shutdown-on-violation to hardware disable an interface when a BPDU is received and the port is disabled.

- **err-disable**
  - Enter the keywords err-disable to enable the port to be put into the error-disable state (EDS) if an error condition occurs.

- **vlan vlan-range**
  - Enter the keyword vlan then the VLAN numbers. The range is from 1 to 4094.

- **cost number**
  - Enter the keyword cost then the port cost value. The range is from 1 to 200000.
  - Defaults:
    - 100 Mb/s Ethernet interface = 200000.
    - 1-Gigabit Ethernet interface = 20000.
    - 10-Gigabit Ethernet interface = 2000.
    - Port Channel interface with one 100 Mb/s Ethernet = 200000.
    - Port Channel interface with one 1 Gigabit Ethernet = 20000.
    - Port Channel interface with one 10 Gigabit Ethernet = 2000.
    - Port Channel with two 1 Gigabit Ethernet = 18000.
    - Port Channel with two 10 Gigabit Ethernet = 1800.
    - Port Channel with two 100 Mbps Ethernet = 180000.

- **priority value**
  - Enter the keyword priority then the Port priority value in increments of 16. The range is from 0 to 240. The default is 128.

- **loopguard**
  - (C-, S-, and E-Series only) Enter the keyword loopguard to enable loop guard on a PVST+ port or port-channel interface.

- **rootguard**
  - (C-, S-, and E-Series only) Enter the keyword rootguard to enable root guard on a PVST+ port or port-channel interface.
BPDU guard option prevents the port from participating in an active STP topology if a BPDU is received 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 is received, and a message is logged so that the administrator can take corrective action.

**NOTE:** A port configured as an edge port, on a PVST switch, immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If you do not enable shutdown-on-violation, BPDUs are still sent to the route process module (RPM) CPU.

You cannot enable root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: % Error: RootGuard is configured. Cannot configure LoopGuard.

When used in a PVST+ network, loop guard is performed per-port or per-port channel at a VLAN level. If no BPDUs are received on a VLAN interface, the port or port-channel transitions to a Loop-Inconsistent (blocking) state only for this VLAN.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
• If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

Example

Dell(conf-if-gi-1/1)# spanning-tree pvst vlan 3 cost 18000
Dell(conf-if-gi-1/1)# end
Dell(conf-if-gi-1/1)# show config
!
interface GigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-gi-1/1)#end
Dell#

Related Commands
• show spanning-tree pvst — views the PVST+ configuration.

spanning-tree pvst err-disable

Place ports in an Err-Disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

S3048

Syntax
spanning-tree pvst err-disable cause invalid-pvst-bpdu

Defaults
Enabled; ports are placed in the Err-Disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

Command Modes
INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information
Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.
Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, Dell Networking OS places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent Dell Networking OS from executing this action, use the `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.

**S3048**

Syntax

```
tc-flush-standard
```

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S3048-ON and S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5(1.0)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

Usage Information

By default, Dell Networking OS implements an optimized flush mechanism for PVST+. This implementation helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this knob command on to enable flushing MAC addresses after receiving every topology change notification.
**vlan bridge-priority**

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

### S3048

**Syntax**

```
vlan vlan-range bridge-priority value
```

To return to the default value, use the no vlan bridge-priority command.

**Parameters**

- `vlan vlan-range`: Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
- `bridge-priority value`: Enter the keywords `bridge-priority` then the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

**Defaults**

**32768**

**Command Modes**

`CONFIGURATION (conf-pvst)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(.19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(.11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(.7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2(1.1)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `vlan forward-delay` — changes the time interval before Dell Networking OS transitions to the Forwarding state.
- `vlan hello-time` — change the time interval between BPDUs.
- `vlan max-age` — changes the time interval before PVST+ refreshes.
- `show spanning-tree pvst` — displays the PVST+ configuration.
**vlan forward-delay**

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

### S3048

**Syntax**

```
vlan vlan-range forward-delay seconds
```

To return to the default setting, use the `no vlan forward-delay` command.

**Parameters**

- **vlan vlan-range**
  - Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.

- **forward-delay seconds**
  - Enter the keywords `forward-delay` then the time interval, in seconds, that Dell Networking OS waits before transitioning PVST+ to the forwarding state. The range is from 4 to 30 seconds. The default is **15 seconds**.

**Defaults**

**15 seconds**

**Command Modes**

`CONFIGURATION (conf-pvst)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2(1.1)</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `vlan bridge-priority` — sets the bridge-priority value.
- `vlan hello-time` — changes the time interval between BPDUs.
- `vlan max-age` — changes the time interval before PVST+ refreshes.
- `show spanning-tree pvst` — displays the PVST+ configuration.
**vlan hello-time**

Set the time interval between generation of PVST+ BPDUs.

**S3048**

**Syntax**

```
vlan vlan-range hello-time seconds
```

To return to the default value, use the no vlan hello-time command.

**Parameters**

- **vlan vlan-range**
  - Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.

- **hello-time seconds**
  - Enter the keywords `hello-time` then the time interval, in seconds, between transmission of BPDUs. The range is from 1 to 10 seconds. The default is **2 seconds**.

**Defaults**

**2 seconds**

**Command Modes**

`CONFIGURATION (conf-pvst)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `vlan bridge-priority` — sets the bridge-priority value.
- `vlan forward-delay` — changes the time interval before Dell Networking OS transitions to the forwarding state.
- `vlan max-age` — changes the time interval before PVST+ refreshes.
- `show spanning-tree pvst` — displays the PVST+ configuration.
**vlan max-age**

To maintain configuration information before refreshing that information, set the time interval for the PVST+ bridge.

### S3048

**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 Dell Networking OS waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

**Defaults**

- **20 seconds**

**Command Modes**

- **CONFIGURATION (conf-pvst)**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `vlan bridge-priority` — sets the bridge-priority value.
- `vlan forward-delay` — changes the time interval before Dell Networking OS transitions to the forwarding state.
- `vlan hello-time` — changes the time interval between BPDUs.
- `show spanning-tree pvst` — displays the PVST+ configuration.
Quality of Service (QoS)

The Dell Networking OS commands for quality of service (QoS) include traffic conditioning and congestion control. QoS commands are not universally supported on all Dell Networking products, platform.

Topics:
- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands
- DSCP Color Map Commands

Global Configuration Commands

There is only one global configuration QoS command.

qos-rate-adjust

By default, while rate limiting, policing, and shaping, Dell Networking OS does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

S3048-ON

Syntax
qos-rate-adjustment overhead-bytes

Parameters
overhead-bytes Include a specified number of bytes of packet overhead to include in rate limiting, policing, and shaping calculations. The range is from 1 to 31.

Defaults
QoS rate adjustment is disabled by default.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
**Usage Information**

By default, when rate policing and shaping, the system does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations.

## 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.

**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**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.
When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the dot1p-priority command to individual interfaces in a port channel.

**rate police**

Police the incoming traffic rate on the selected interface.

**S3048-ON**

**Syntax**

```
rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]
```

**Parameters**

- `kbps`: Enter the keyword kbps to specify the rate limit in Klobits per second (Kbps). The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
- `committed-rate`: Enter the bandwidth in Mbps. The range is from 0 to 40000.
- `burst-KB`: (OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is 50.
- `peak peak-rate`: (OPTIONAL) Enter the keyword peak then a number to specify the peak rate in Mbps. The range is from 0 to 40000.
- `vlan vlan-id`: (OPTIONAL) Enter the keyword vlan then a VLAN ID to police traffic to those specific VLANs. The range is from 1 to 4094.

**Defaults**

Granularity for committed-rate and peak-rate is Mbps unless you use the kbps option.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added the kbps option on the C-Series, E-Series, and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
rate shape
Shape the traffic output on the selected interface.

**S3048-ON**

**Syntax**
```
rate shape [kbps] rate [burst-KB]
```

**Parameters**
- **kbps**: Enter the keyword kbps to specify the rate limit in Kilobits per second (Kbps). Enter the value in multiples of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
- **rate**: The range is from 10 to 40000.
- **burst-KB**: (OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is 50.

**Defaults**
Granularity for rate is Mbps unless you use the kbps option.

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.2.1.0 | Added the kbps option on the C-Series, E-Series, and S-Series.
7.6.1.0 | Introduced on the S-Series and C-Series.

**Usage Information**
- **NOTE**: Per Port rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate police is supported on only tagged ports with Layer 2 switched traffic.

**S-Series**
On one interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface.

**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.
Version Description
6.1.1.1 Introduced on the E-Series.

Usage Information
If traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured.

On 40-port 10G stack-unit if the traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured.

**NOTE:** When packets of size greater than 7000 bytes are expected to be received from the network, Dell Networking recommends that you configure the burst value to be more than 175 KB if you configured the rate shape. Such a setting ensures proper bandwidth sharing across queues.

Related Commands
- `rate-shape` — shapes traffic output as part of the designated policy.

**service-class dot1p-mapping**

Configure a service-class criterion based on a dot1p value.

**S3048-ON**

**Syntax**
```
service-class dot1p-mapping {dot1p0 queue | dot1p1 queue | dot1p2 queue | dot1p3 queue | dot1p4 queue | dot1p5 queue | dot1p6 queue | dot1p7 queue}
```

**Parameters**
- `queue` Enter a value from 0 to 7.

**Defaults**
For each dot1p Priority, the default CoS queue value is:
- Dot1p Priority : 0 1 2 3 4 5 6 7

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Quality of Service (GoS) | 1181
Usage Information
To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

Related Commands
- `show qos dot1p-queue-mapping` — displays the dot1p priority to queue mapping on the switch.

---

**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.

**S3048-ON**

**Syntax**

```
service-class dynamic dot1p
```

To return to the default setting, use the `no service-class dynamic dot1p` command.

**Defaults**

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

<table>
<thead>
<tr>
<th>dot1p</th>
<th>Queue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

**Command Modes**

- `INTERFACE`
- `CONFIGURATION`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
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.

**strict-priority queue**

Configure a unicast queue as a strict-priority (SP) queue.

**S3048-ON**

**Syntax**

```
strict-priority queue unicast number
```

**Parameters**

- `unicast number`
  Enter the keyword `unicast` then the queue number. The range is from 1 to 3.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(0.0P6)  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.
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.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify data traffic into one of eight classes. Dell Networking OS enables you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANS, or loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

S3048-ON

Syntax

bandwidth-percentage percentage

To remove the bandwidth percentage, use the no bandwidth-percentage command.

Parameters

percentage

Enter the percentage assignment of bandwidth to the class/queue. The range is from 1 to 100% (granularity 1%).

Defaults

none

Command Modes

CONFIGURATION (conf-qos-policy-out)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.1.9.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
class-map

Create/access a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

S3048-ON

class-map {match-all | match-any} class-map-name [cpu-qos] [layer2]

Parameters

- **match-all**
  Determines how packets are evaluated when multiple match criteria exist. Enter the keywords match-all to determine that the packets must meet all the match criteria in order to be a member of the class.

- **match-any**
  Determines how packets are evaluated when multiple match criteria exist. Enter the keywords match-any to determine that the packets must meet at least one of the match criteria in order to be a member of the class.

- **class-map-name**
  Enter a name of the class for the class map in a character format (32 character maximum).

- **cpu-qos**
  Enter the keyword cpu-qos to assign this Class Map to control plane traffic only (CoPP).

- **layer2**
  Enter the keyword layer2 to specify a Layer 2 Class Map. The default is Layer 3.

Defaults

Layer 3

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
# clear qos statistics

Clear qos statistics clears statistics from show qos statistics.

## S3048–ON

### Syntax

clear qos statistics interface-name

### Parameters

- **interface-name**
  - Enter one of the following keywords:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

### Defaults

none

### Command Modes

- EXEC
- EXEC Privilege
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.18.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands
- `show qos statistics` — displays the QoS statistics.

**description**

Add a description to the selected policy map or QoS policy.

**S3048-ON**

**Syntax**
```
description {description}
```
To remove the description, use the `no description {description}` command.

**Parameters**
- `description` Enter a description to identify the policies (80 characters maximum).

**Defaults**
- none

**Command Modes**
- CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

**NOTE:** IPv6 class-maps and IP-any class-maps do not match. This condition is true for IPv6 and IP-any class-maps on both ACLs as well as VLANs.

**S3048-ON**

**Syntax**

```plaintext
match ip access-group access-group-name [set-ip-dscp value | set-color value]
```

To remove ACL match criteria from a class map, use the ```no match ip access-group access-group-name [set-ip-dscp value | set-color value]``` command.

**Parameters**

- `access-group-name` Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the class-map specifies.
- `set-ip-dscp value` (OPTIONAL) Enter the keywords ```set-ip-dscp``` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.
- `set-color value` (Optional) Enter the keyword ```set-color``` followed by a color value. Traffic that fulfills the match criteria is marked with the color value that you specify. The default value is Yellow.

**Defaults**

None

**Command Modes**

CLASS-MAP CONFIGURATION (config-class-map)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the DSCP Marking option support on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series; added support for the DSCP Marking option.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
To access this command, enter the class-map command. After the class map is identified, you can configure the match criteria. For class-map match-any, a maximum of five ACL match criteria are allowed. For class-map match-all, only one ACL match criteria is allowed.

**Related Commands**
- `class-map` — identifies the class map.

---

**match ip dscp**

Use a differentiated services code point (DSCP) value as a match criteria.

**S3048-ON**

**Syntax**
```
match {ip | ipv6 | ip-any} dscp dscp-list [set-ip-dscp value]
```

To remove a DSCP value as a match criteria, use the `no match {ip | ipv6 | ip-any} dscp dscp-list [[multicast] set-ip-dscp value]` command.

**Parameters**
- `ip` Enter the keyword `ip` to support IPv4 traffic.
- `ipv6` Enter the keyword `ipv6` to support IPv6 traffic.
- `ip-any` Enter the keyword `ip-any` to support IPv4 and IPv6 traffic.
- `dscp-list` Enter the IP DSCP values that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 63.
- `set-ip-dscp value` (OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

**Defaults**
- none

**Command Modes**
- CLASS-MAP CONFIGURATION (config-class-map)
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added the <code>ipv6</code> and <code>ip-any</code> options on the Z9000, S6000, S4820T, S4810, MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the keyword <code>multicast</code>; added the DSCP Marking option support on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series; added support for the DSCP Marking option.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip dscp` and `match ip precedence` commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7, enter either the `match ip dscp 0,1,2,3,4,5,6,7` or `match ip dscp 0-7` command.

**NOTE:** Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values must match.

Related Commands

- `class-map` — identifies the class map.

### match ip precedence

Use IP precedence values as a match criteria.

**S3048-ON**

**Syntax**

```
match {ip | ipv6 | ip-any} precedence ip-precedence-list [set-ip-dscp value]
```

To remove IP precedence as a match criteria, use the `no match {ip | ipv6 | ip-any} precedence ip-precedence-list [[multicast] set-ip-dscp value]` command.
Parameters

- **ip** Enter the keyword ip to support IPv4 traffic.
- **ipv6** Enter the keyword ipv6 to support IPv6 traffic.
- **ip-any** Enter the keyword ip-any to support IPv4 and IPv6 traffic.
- **ip-precedence-list** Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1, 2, 3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 7.
- **set-ip-dscp value** (OPTIONAL) Enter the keywords set-ip-dscp then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults

- none

Command Modes

- CLASS-MAP CONFIGURATION (config-class-map)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for the ipv6 and ip-any options on the Z9000, S6000, S4820T, S4810, MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Added the keyword multicast. Added support for the DSCP Marking option for the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series. Added support for the DSCP Marking option.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To access this command, enter the class-map command. After the class map is identified, you can configure the match criteria.

The **match ip precedence** command and the **match ip dscp** command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3, enter either the **match ip precedence 0-3** or **match ip precedence 0,1,2,3** command.
NOTE: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values must match.

Related Commands
- `class-map` — identifies the class map.

**match ip vlan**

Uses a VLAN as the match criterion for an L3 class map.

**S3048-ONS3048-ON**

**Syntax**
```
match ip vlan vlan-id
```

To remove VLAN as the match criterion, use the `no match ip vlan vlan-id` command.

**Parameters**
- `vlan vlan-id` Enter the keyword `vlan` and then the ID of the VLAN. The range is from 1 to 4094.

**Defaults**
None.

**Command Modes**
`CONF-CLASS-MAP`

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**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.

**S3048-ON**

**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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5.(0.1) Introduced on the Z9500.
9.4.(0.0) Introduced on the S-Series and Z-Series.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Use this command to match an IP class-map against a single VRF ID.

Related Commands

- `class-map` — identifies the class map.

**match mac access-group**

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

**S3048-ON**

Syntax

`match mac access-group {mac-acl-name}`

Parameters

`mac-acl-name` Enter a MAC ACL name. Its contents is used as the match criteria in the class map.

Defaults

none

Command Modes

CLASS-MAP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the Z9500.
9.2(1.0) Introduced on the S6000.
9.0.2.0 Introduced on the S6000.
match mac dot1p

Configure a match criterion for a class map based on a dot1p value.

**S3048-ON**

```plaintext
Syntax:
match mac dot1p (dot1p-list)

Parameters:
dot1p-list: Enter a dot1p value. The range is from 0 to 7.

Defaults:
one

Command Modes:
CLASS-MAP

Command History:
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Available on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for the DSCP Marking option.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
```
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.

**S3048-ON**

**Syntax**

```
match mac vlan number
```

**Parameters**

- `number` Enter the VLAN ID. The range is from 1 to 4094.

**Defaults**

none

**Command Modes**

CLASS-MAP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced.</td>
</tr>
</tbody>
</table>

**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 (output) applied on an interface.

### S3048-ON

**Syntax**

```
policy-aggregate qos-policy-name
```

To remove a policy aggregate configuration, use the `no policy-aggregate qos-policy-name` command.

**Parameters**

- `qos-policy-name` Enter the name of the policy map in character format (32 characters maximum).

**Defaults**

none

**Command Modes**

CONFIGURATION (policy-map-input and policy-map-output)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Policy name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

An aggregate output QoS policy applies to all outbound port traffic. An aggregate output QoS policy can coexist with per-queue output QoS policies. If the rate shape exists in both aggregate and per-queue qos-policy, minimum of 2 take effect. Some of all Queue-rate will not exceed aggregate.

**Related Commands**

- `policy-map-input` — creates an input policy map.
- `policy-map-output` — creates an output policy map.
policy-map-input

Create an input policy map.

S3048-ON

Syntax

policy-map-input policy-map-name cpu-qos | [layer2] [cpu-qos]

To remove an input policy map, use the no policy-map-input policy-map-name cpu-qos | [layer2] [cpu-qos] command.

Parameters

- **policy-map-name**: Enter the name of the policy map in character format (32 characters maximum).
- **cpu-qos**: Enter the cpu-qos keyword to assign this ACL to control plane traffic only.
- **layer2** (OPTIONAL): Enter the keyword layer2 to specify a Layer 2 Class Map. The default is Layer 3.
- **cpu-qos** (OPTIONAL): Enter the keyword cpu-qos to create an input policy to be used to rate-limit control-plane traffic (CoPP).

Defaults

Layer 3

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Policy name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Expanded to add support for Layer 2.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or incoming packets DSCP. This command enables Policy-Map-Input Configuration mode (conf-policy-map-in). When you configure an input policy map for CoPP, you must enter the keyword cpu-qos.
**Related Commands**

- `service-queue` — assigns a class map and QoS policy to different queues.
- `service-policy input` — applies an input policy map to the selected interface.

---

**policy-map-output**

Create an output policy map.

### S3048-ON

**Syntax**

```plaintext
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Policy name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.

**S3048-ON**

**Syntax**

```
qos-policy-input qos-policy-name cpu-qos | layer2
```

To remove an existing input QoS policy from the router, use the `no qos-policy-input qos-policy-name cpu-qos | layer2` command.

**Parameters**

- **qos-policy-name**
  - Enter the name for the policy map in character format (32 characters maximum).

- **cpu-qos**
  - (OPTIONAL) Enter the keyword `cpu-qos` keyword to assign this ACL to control plane traffic only.

- **layer2**
  - (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is Layer 3.

**Defaults**

Layer 3

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Policy name character limit increased from 16 to 32.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1(1.1)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Use this command to specify the name of the input QoS policy. Once input policy is specified, rate-police can be defined. This command enables the qos-policy-input configuration mode— (conf-qos-policy-in).
When changing a Service-Queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the show qos statistics command is reset.

If you create create a QoS input policy to be used for CoPP, you must enter the keyword cpu-qos.

Related Commands

- rate police — incoming traffic policing function.

**qos-policy-output**

Create a QoS output policy.

**S3048-ON**

**Syntax**

```plaintext
qos-policy-output qos-policy-name
```

To remove an existing output QoS policy, use the `no qos-policy-output qos-policy-name` command.

**Parameters**

- **qos-policy-name** Enter your output QoS policy name in character format (32 characters maximum).

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.2.1.0 | Policy name character limit increased from 16 to 32.
7.6.1.0 | Introduced on the C-Series and S-Series.
6.1.1.1 | Introduced on the E-Series.

**Usage Information**

Use this command to specify the name of the output QoS policy. Once output policy is specified, rate-shape, scheduler strict, bandwidth-percentage, and WRED can be defined. This command enables the qos-policy-output configuration mode—(conf-qos-policy-out).
Related Commands

- bandwidth-percentage — assigns percentage of bandwidth to the class/queue.
- wred — assigns yellow or green drop precedence.

queue egress

Assign a WRED Curve to all eight egress Multicast queues or designate the percentage for the Multicast bandwidth queue.

**Syntax**

```
queue egress multicast linecard {slot number port-set number | all} [wred-profile name | multicast-bandwidth percentage]
```

To return to the default, use the `no queue egress multicast linecard {slot number port-set number | all} [wred-profile name | multicast-bandwidth percentage]` command.

**Parameters**

- `linecard number` (Required) Enter the keyword `linecard` then the line card slot number.
- `port-set number` Enter the keywords `port-set` then the line card’s port pipe. The range is from 0 or 1.
- `all` Enter the keyword `all` to apply to all line cards.
- `wred-profile name` (Optional) Enter the keywords `wred-profile` then your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names.

Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

- `multicast-bandwidth percentage` (Optional) Enter the keywords `multicast-bandwidth` then the bandwidth percentage. The range is from 0 to 100%.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(0.0P5)
- 9.8(0.0P2)
- 8.3.19.0
- 8.3.8.10
- 7.5.1.0
- 7.4.1.0 and 6.5.3.0

**Usage Information**

This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED curve is applied to all eight egress Multicast queues.

**Important Points to Remember — Multicast-Bandwidth Option**

- A unique multicast weighted fair queuing (WFQ) setting can be applied only on a per port-pipe basis. The minimum percentage of the multicast bandwidth assigned to any of the ports in the port-pipe takes effect for the entire port-pipe.
- If the percentage of multicast bandwidth is 0, control traffic going through multicast queues are dropped.
• The `no` form of the command without `multicast-bandwidth` and `wred-profile`, removes both the `wred-profile` and `multicast-bandwidth` configuration.
• On 10-Gigabit ports only, the `multicast-bandwidth` option works only if the total `unicast bandwidth` is more than the `multicast bandwidth`.
• If `strict priority` is applied along with `multicast-bandwidth`, the effect of `strict priority` is on all ports where `unicast` and `multicast bandwidth` are applied.
• When `multicast bandwidth` is assigned along with `unicast bandwidth`, first `multicast bandwidth` is reserved for that port, then the remaining `unicast bandwidth` configured is adjusted according to the `bandwidth available` after reserving for `multicast bandwidth`.

**queue ingress**

Assign a WRED Curve to all eight ingress Multicast queues or designate the percentage for the Multicast bandwidth queue.

**Syntax**
```
queue ingress multicast {linecard slot number port-set number | all} [wred-profile name]
```

To return to the default, use the `no queue ingress multicast {linecard slot number port-set number | all} [wred-profile name]` command.

**Parameters**
- **linecard number**
  - Enter the keyword `linecard` then the line card slot number.
- **port-set number**
  - Enter the keywords `port-set` then the line card's port pipe. The range is from 0 or 1.
- **all**
  - Enter the keyword `all` to apply to all line cards.
- **wred-profile name**
  - (OPTIONAL) Enter the keywords `wred-profile` then your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names.

Pre-defined Profiles: `wred_drop`, `wred-ge_y`, `wred_ge_g`, `wred_teng_y`, `wred_teng_g`.

**Defaults**
- none

**Command Modes**
- CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**
- 9.8(0.0P5)
  - Introduced on the S4048-ON.
- 9.8(0.0P2)
  - Introduced on the S3048-ON.
- 8.3.19.0
  - Introduced on the S4820T.
- 8.3.8.0
  - Introduced on the S4810.
- 7.4.1.0 and 6.5.3.0
  - Introduced on the E-Series.

**Usage Information**
This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED Curve is applied to all eight ingress Multicast queues.

**NOTE:** The `multicast-bandwidth` option is not supported on queue ingress. If you attempt to use the `multicast-bandwidth` option, the following reject error message is generated:

```
%Error:Bandwidth-percent is not allowed for ingress multicast.
```
**rate-police**

Specify the policing functionality on incoming traffic.

### S3048-ON

**Syntax**

```plaintext
rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]
```

**Parameters**

- **kbps**
  - Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
  - **committed-rate**
    - Enter the bandwidth in Mbps. The range is from 0 to 40000.
  - **burst-KB**
    - (OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is 100.
  - **peak peak-rate**
    - (OPTIONAL) Enter the keyword `peak` then a number to specify the peak rate in Mbps. The range is from 0 to 40000. The default is the same as designated for `committed-rate`.

**Defaults**

- Burst size is 100KB. `peak-rate` is by default the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

**Command Modes**

QOS-POLICY-IN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added the <code>kbps</code> option on the C-Series, E-Series, and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.11</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The default burst size is 100Kb. If a different value is required, you must configure the burst size to the required value.
rate-shape

Shape traffic output as part of the designated policy.

**S3048-ON**

**Syntax**

```
```

**Parameters**

- `pps`
  - Enter the keyword `pps` to specify the rate limit in packets per second (pps).
- `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).
- `burst-kbps`
  - (OPTIONAL) Enter the burst size in KB. The range is from 0 to 40000. The default is 100.
- `burst-packets`
  - Enter the peak rate or committed rate burst size in packets per seconds.

**Defaults**

Burst size is 10KB. Granularity for rate is Mbps unless you use the `kbps` option.

**Command Modes**

QOS-POLICY-OUT

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added the kbps option on the C-Series, E-Series, and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

On 40-port 10G stack-unit if the traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured. You must configure the peak rate and peak burst size using the same value: kilobits or packets per second. Similarly, you must configure the committed rate and committed burst size with the
same measurement. Peak rate refers to the maximum rate for traffic arriving or exiting an interface under normal traffic conditions. Peak burst size indicates the maximum size of unused peak bandwidth that is aggregated. This aggregated bandwidth enables brief durations of burst traffic that exceeds the peak rate and committed burst. Committed rate refers to the guaranteed bandwidth for traffic entering or leaving the interface under normal network conditions. When traffic propagates at an average rate that is less than or equal to the committed rate, it is considered to be green-colored or coded. When the transmitted traffic falls below the committed rate, the bandwidth, which is not used by any traffic that is traversing the network, is aggregated to form the committed burst size. Traffic is considered to be green-colored up to the point at which the unused bandwidth does not exceed the committed burst size.

Related Commands
- `rate shape` — shapes traffic output as part of the designated policy.
- `qos-policy-output` — creates a QoS output policy.

service-policy input

Apply an input policy map to the selected interface.

S3048-ON

Syntax
```
service-policy input policy-map-name [layer2]
```

To remove the input policy map from the interface, use the `no service-policy input policy-map-name [layer2]` command.

Parameters
- `policy-map-name` Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.
- `layer2` (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is `Layer 3`.

Defaults
- Layer 3

Command Modes
- INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
service-policy output

Apply an output policy map to the selected interface.

S3048–ON

device

Syntax

```
service-policy output policy-map-name
```

To remove the output policy map from the interface, use the `no service-policy output policy-map-name` command.

Parameters

- `policy-map-name` Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.

Usage Information

You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

**Note:** The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface. However, the `service-policy input` command (without the `policy-map-name` option) and the `service-class dynamic dot1p` command are allowed on an interface.

Related Commands

- `policy-map input` — creates an input policy map.
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.

**S3048-ON**

**Syntax**

```
service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]
```

To remove the queue assignment, use the `no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]` command.

**Parameters**

- `queue-id`:
  Enter the value used to identify a queue. The range is from 0 to 7.

- `class-map class-map-name`:
  (OPTIONAL) Enter the keyword `class-map` then the class map name assigned to the queue in character format (32 character maximum).

  **NOTE:** This option is available under `policy-map-input` only.

- `qos-policy qos-policy-name`:
  (OPTIONAL) Enter the keywords `qos-policy` then the QoS policy name assigned to the queue in text format (32 characters maximum). This specifies the input QoS policy assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

**Defaults**

none

**Command Modes**

CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(1.0)
- 9.8(0.0P5)
- 9.8(0.0P2)
- 9.7(0.0)
- 9.2(1.0)
- 9.0(2.0)
- 8.3.19.0
- 8.3.11.1

**Description**

- Introduced on the Z9100-ON.
- Introduced on the S4048-ON.
- Introduced on the S3048-ON.
- Introduced on the S6000-ON.
- Introduced on the Z9500.
- Introduced on the S6000.
- Introduced on the S4820T.
- Introduced on the Z9000.
set

Mark outgoing traffic with a differentiated service code point (DSCP) or dot1p value.

**S3048-ON**

**Syntax**

set (ip-dscp value | mac-dot1p value)

**Parameters**

- **ip-dscp value** (OPTIONAL) Enter the keywords ip-dscp then the IP DSCP value. The range is from 0 to 63.
- **mac-dot1p value** Enter the keywords mac-dot1p then the dot1p value. The range is from 0 to 7.

**Defaults**

none

**Command Modes**

CONFIGURATION (conf-qos-policy-in)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added mac-dot1p on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
show qos class-map

View the current class map information.

S3048–ON

Syntax

show qos class-map [class-name]

Parameters

class-name (Optional) Enter the name of a configured class map.

Defaults

none

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.1.1.1 Introduced on the E-Series.

Example

Dell# show qos class-map
Class-map match-any CM
show qos dot1p-queue-mapping

Displays the dot1p priority to queue mapping on the switch.

Syntax

show qos dot1p-queue-mapping

Defaults

- dot1p Priority: 0 1 2 3 4 5 6 7
- Queue: 1 0 1 2 3 3

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information

trust dot1p, dot1p-priority, service-class dynamic dot1; all these features work over the mapping in this command output.

Related Commands

- service-class dot1p-mapping — Identifies the class map.

show qos policy-map

View the QoS policy map information.

S3048–ON

Syntax

show qos policy-map {summary [interface] | detail}

Parameters

9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
To view a policy map interface summary, enter the keyword `summary` and optionally one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

To view a policy map interface in detail, enter the keyword `detail` and optionally one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series only: Added <code>trust IPv6 diffserv</code>.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example (IPv4)**

```bash
Dell# show qos policy-map detail gigabitethernet 1/1

Interface GigabitEthernet 4/1
Policy-map-input policy
Trust dffserv
Queue# Class-map-name Qos-policy-name
  0 - q0
  1  CM1 q1
  2  CM2 q2
```
show qos policy-map-input

View the input QoS policy map details.

S3048–ON

Syntax

show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]

Parameters

- **policy-map-name**: Enter the policy map name.
- **class class-map-name**: Enter the keyword class then the class map name.
- **qos-policy-input qos-policy-name**: Enter the keyword qos-policy-input then the QoS policy name.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
show qos policy-map-output

View the output QoS policy map details.

S3048-ON

**Syntax**

```
show qos policy-map-output [policy-map-name] [qos-policy-output qos-policy-name]
```

**Parameters**

- `policy-map-name` Enter the policy map name.
- `qos-policy-output` Enter the keyword qos-policy-output then the QoS policy name.
- `qos-policy-name` Enter the QoS policy name.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>

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#
```

```
Dell# show qos policy-map-input
Policy-map-input pmap1
Trust ipv6-diffserv
Queue# Class-map-name Qos-policy-name
  0       c0              q0
  1       c1              q1
  2       c2              q2
  3       c3              q3
  4       c4              q4
  5       c5              -
  6       c6              q6
  7       c7              q7
Dell#
```
show qos 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Example

Dell# show qos policy-map-output
Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue# Qos-policy-name
   0  qosPolicyOutput
Dell#
show qos qos-policy-output

View the output QoS policy details.

S3048–ON

Syntax

show qos qos-policy-output [qos-policy-name]

Parameters

qos-policy-name Enter the QoS policy name.

Defaults

none

Command Modes

• EXEC
• EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3(19.0) Introduced on the S4820T.
8.3(11.1) Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the C-Series and S-Series.
show qos statistics

View QoS statistics.

S3048–ON

Syntax

show qos statistics {egress-queue [interface]} | {wred-profile [interface]} | [interface]

Parameters

egress-queue

interface

Enter the keyword egress-queue to display the egress-queue statistics and optionally one of the following keywords and slot/port or number information.

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

wred-profile

interface

Enter the keywords wred-profile and optionally one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

interface

Enter one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Example

Dell# show qos qos-policy-output
Qos-policy-output qosOut
  Rate-limit 50 50 peak 50 50
  Wred yellow 1
  Wred green 1
Dell#
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.
9.8(0.0) | Added the egress-queue keyword.
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.
7.7.1.1 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.1.1.1 | Introduced on the E-Series.

Example

Dell# show qos statistics gi 1/1

<table>
<thead>
<tr>
<th>Queue#</th>
<th>Queued Bytes (Cumulative)</th>
<th>Queued Pkts (Cumulative)</th>
<th>Matched Bytes (Cumulative)</th>
<th>Matched Pkts (Cumulative)</th>
<th>Dropped Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1883725</td>
<td>1883725000</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>1883724</td>
<td>1883724000</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>1883720</td>
<td>1883720000</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>1883720</td>
<td>1883720000</td>
<td>0</td>
</tr>
</tbody>
</table>

Dell#

Usage Information

The following list describes output of the `show qos statistics` command in the example:

- **Queue #** — Queue Number.
- **Queued Bytes** — Snapshot of the byte count in that queue.
- **Queued Pkts** — Cumulative packet count in that queue.
- **Matched Pkts** — The number of packets that matched the class-map criteria.

**NOTE:** When you configure trust, matched packet counters are not incremented in this field.

- **Matched Bytes** — The number of bytes that matched the class-map criteria.

**NOTE:** When you configure trust, matched byte counters are not incremented in this field.

- **Dropped Pkts** — The total of the number of packets dropped for green, yellow and out-of-profile.
**show qos wred-profile**

View the WRED profile details.

**S3048-ON**

**Syntax**

```
show qos wred-profile wred-profile-name
```

**Parameters**

- `wred-profile-name` Enter the WRED profile name to view the profile details.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show qos wred-profile
Wred-profile-name min-threshold max-threshold max-drop-rate
wred_drop 0 0 100
wred_gig_y 467 4671 100
wred_gig_g 467 4671 50
wred_teng_y 467 4671 50
wred_teng_g 467 4671 25
Dell#
```
test cam-usage

Check the Input Policy Map configuration for the CAM usage.

S3048-ON

test cam-usage service-policy input policy-map stack-unit {
  [number port-set portpipe number] | [all]}

Syntax

Parameters

- **policy-map**: Enter the policy map name.
- **stack-unit number**: (OPTIONAL) Enter the keyword stack-unit then the stack-unit slot number.
- **port-set portpipe number**: Enter the keywords port-set then the stack-unit port pipe number. The range is from 0 or 1.
- **stack-unit all**: (OPTIONAL) Enter the keywords stack-unit all to indicate all stack-unit.

Defaults

- none

Command Modes

- EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information

- This feature allows you to determine if the CAM has enough space available before applying the configuration on an interface.

  An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column contains the size of the CAM space required for the Trust rule and not the Class-map rule.

  The following describes the `test cam-usage service-policy input policy-map stack-unit` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stack-unit</td>
<td>Indicates the stack-unit slot number.</td>
</tr>
<tr>
<td>Portpipe</td>
<td>Indicates the portpipe number.</td>
</tr>
<tr>
<td>CAM Partition</td>
<td>The CAM space where the rules are added.</td>
</tr>
</tbody>
</table>
### Field Description

**Available CAM** Indicates the free CAM space, in the partition, for the classification rules.

**NOTE:** The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, cannot be used as a policy map for the classification rules.

**Estimated CAM per Port** Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface.

**NOTE:** The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.

**Status (Allowed ports)** Indicates if the input policy map configuration on an interface belonging to a stack-unit/port-pipe is successful — Allowed (n) — or not successful — Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.

**NOTE:** In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed; therefore, the output contains only L2ACL CAM partition entries.

### Example

```
Dell# test cam-usage service-policy input pmap_l2 stack-unit all

For a L2 Input Policy Map pmap_l2, the output must be as follows,

| stack-unit | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port | Status (Allowed ports)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>L2ACL</td>
<td>500</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>L2ACL</td>
<td>100</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>L2ACL</td>
<td>1000</td>
<td>200</td>
<td>Allowed (5)</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>L2ACL</td>
<td>0</td>
<td>200</td>
<td>Exception</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>L2ACL</td>
<td>400</td>
<td>200</td>
<td>Allowed (2)</td>
</tr>
</tbody>
</table>
```

### threshold

Specify the minimum and maximum threshold values for the configured WRED profiles.

#### S3048-ON

**Syntax**

```
threshold min number max number max-drop-drop
```

To remove the threshold values, use the `no threshold min number max number` command.

**Parameters**

- **min number** Enter the keyword `min` then the minimum threshold number for the WRED profile. The range is from 1 to 9360.
max number

Enter the keyword `max` then the maximum threshold number for the WRED profile. The range is from 1 to 9360 KB.

max-drop-drop number

Enter the keyword `max-drop-drop` followed by the maximum number of packets for the WRED profile. The range is from 0 to 100 KB.

Defaults

none

Command Modes

CONFIGURATION (config-wred)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.8.0 Introduced on the S4810.
6.1.1.1 Introduced on the E-Series.

Usage Information

To configure the minimum and maximum threshold values for user-defined profiles, use this command. Additionally, to modify the minimum and maximum threshold values for the pre-defined WRED profiles, use this command. If you delete the threshold values of the pre-defined WRED profiles, the profiles revert to their original default values.

<table>
<thead>
<tr>
<th>Pre-Defined WRED Profile Name</th>
<th>Minimum Threshold</th>
<th>Maximum Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>wred_drop</td>
<td>0</td>
<td>100</td>
</tr>
<tr>
<td>wred_ten_y</td>
<td>467</td>
<td>4671</td>
</tr>
<tr>
<td>wred_ten_g</td>
<td>467</td>
<td>4671</td>
</tr>
</tbody>
</table>

Related Commands

- `wred-profile` — creates a WRED profile.
trust

Specify dynamic classification (DSCP) or dot1p to trust.

S3048–ON

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 or dot1p value as a secondary option in case no match occurs against the configured class maps.

Defaults

none

Command Modes

CONFIGURATION (conf-policy-map-in)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added fallback to the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added dot1p to the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added dot1p and IPv6 DSCP.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>DSCP/CP hex Range (XXX)</th>
<th>DSCP Definition</th>
<th>Traditional IP Precedence</th>
<th>S6000 Internal Queue ID</th>
<th>S-Series Internal Queue ID</th>
<th>DSCP/CP Decimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>111XXX</td>
<td>Network Control</td>
<td>7</td>
<td>3</td>
<td>48–63</td>
<td></td>
</tr>
<tr>
<td>110XXX</td>
<td>Internetwork Control</td>
<td>6</td>
<td>3</td>
<td>48–63</td>
<td></td>
</tr>
<tr>
<td>101XXX</td>
<td>EF (Expedited Forwarding)</td>
<td>5</td>
<td>2</td>
<td>32–47</td>
<td></td>
</tr>
<tr>
<td>100XXX</td>
<td>AF4 (Assured Forwarding)</td>
<td>4</td>
<td>2</td>
<td>32–47</td>
<td></td>
</tr>
<tr>
<td>011XXX</td>
<td>AF3</td>
<td>3</td>
<td>1</td>
<td>16–31</td>
<td></td>
</tr>
<tr>
<td>010XXX</td>
<td>AF2</td>
<td>2</td>
<td>1</td>
<td>16–31</td>
<td></td>
</tr>
<tr>
<td>001XXX</td>
<td>AF1</td>
<td>1</td>
<td>0</td>
<td>0–15</td>
<td></td>
</tr>
<tr>
<td>000XXX</td>
<td>BE (Best Effort)</td>
<td>0</td>
<td>0</td>
<td>0–15</td>
<td></td>
</tr>
</tbody>
</table>

**wred**

Designate the WRED profile to yellow or green traffic.

**S3048-ON**

**Syntax**

```plaintext
wred {yellow | green} profile-name
```

To remove the WRED drop precedence, use the no wred {yellow | green} [profile-name] command.

**Parameters**

- **yellow | green**
  - Enter the keyword `yellow` for yellow traffic. A DSCP value of `xxx110` and `xxx100`, `xxx101` maps to yellow.
  - Enter the keyword `green` for green traffic. A DSCP value of `xxx0xx` are green and DSCP `11111` are red packets.

- **profile-name**
  - Enter your WRED profile name in character format (32 character maximum). Or use one of the five pre-defined WRED profile names.

  Pre-defined Profiles: wred_drop, wred_ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

**Defaults**

When WRED green is applied, default WRED yellow profiles take effect and vice-versa.

**Command Modes**

CONFIGURATION (conf-qos-policy-out)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**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).

**S3048–ON**

**Syntax**

```
wred ecn
```

To stop marking packets, use the `no wred ecn` command.

**Defaults**

none

**Command Modes**

CONFIGURATION (conf-qos-policy-out)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
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.

**S3048-ON**

**Syntax**

```
wred-profile wred-profile-name
```

To remove an existing WRED profile, use the no wred-profile command.

**Parameters**

- `wred-profile-name` Enter your WRED profile name in character format (32 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles.

  Pre-defined Profiles: wred_drop, wred_ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

**Defaults**

The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined wred_ge_g values.

If green profile is applied, default yellow also take effect and vice-versa.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>6.1.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
Use the default pre-defined profiles or configure your own profile. You cannot delete the pre-defined profiles or their default values. This command enables WRED configuration mode — (conf-wred).

**Related Commands**
- **threshold** — specifies the minimum and maximum threshold values of the WRED profile.

**DSCP Color Map Commands**

The DSCP color map allows you to set the number of specific DSCP values to yellow or red. Traffic marked as yellow delivers traffic to the egress queue which will either transmit the packet if it has available bandwidth or drop the packet due to no ability to send. Traffic marked as red (high drop precedence) is dropped.

**dscp**

Sets the number of specific DSCP values for a color map profile to yellow or red.

**Syntax**
```
dscp {yellow | red} [list-dscp-values]
```

To remove a color policy map profile, use the no dscp {yellow | red} [dscp-list] command.

**Parameters**
- **Yellow**
  - Enter the yellow keyword. Traffic marked as yellow delivers traffic to the egress queue which either transmits the packet if it has available bandwidth or drops the packet due to no ability to send.
- **Red**
  - Enter the red keyword. Traffic marked as red is dropped.
- **dscp-list**
  - Enter a list of IP DSCP values. The dscp-list parameter specifies the full list of IP DSCP value(s) for the specified color. Each DSCP value in a list is separate values by commas – no spaces (1,2,3) or indicates a list of values separated by a hyphen (1-3). Range is 0 to 63.

**Defaults**
- None

**Command Modes**
- CONFIG-COLOR-MAP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
Usage Information
If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

The default setting for each DSCP value (0-63) is green (low drop precedence). This command allows setting the number of specific DSCP values to yellow or red.

Important Points to Remember

- All DSCP values that are not specified as yellow or red are colored green.
- A DSCP value cannot be in both the yellow and red lists. Setting the red or yellow list with any DSCP value that is already in the other list results in an error and no update to that list is made.
- Each color map can only have one list of DSCP values for each color; any DSCP values previously listed for that color that are not in the new DSCP list are colored green.

Example

```
Dell(conf-dscp-color-map)# dscp yellow 9,10,11,13,15,16
```

Related Commands

- `qos dscp-color-map` — configures the DSCP color map.
- `qos dscp-color-policy` — configures a DSCP color policy.

### qos dscp-color-map

Configure the DSCP color map.

**Syntax**

```
qos dscp-color-map map-name
```

To remove a color map, use the `no qos dscp-color-map map-name` command.

**Parameters**

- `map-name` Enter the name of the DSCP color map. The map name can have a maximum of 32 characters.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
A color map outlines the codepoint mappings to the appropriate color mapping (green, yellow, red) for the traffic. The system uses this information to handle the traffic on the interface based on the traffic priority and places it into the appropriate shaping queue. You cannot delete a DSCP color map when it is configured on an interface. If you do, all the DSCP values are set to green (low drop precedence). To delete the DSCP color map that is being used by one or more interfaces, remove the DSCP map from each interface.

Example

Dell(conf)#qos dscp-color-map mymap

Related Commands

- **qos dscp-color-map** — associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map.
- **dscp** — sets the number of specific DSCP values for color map profile to yellow or red.

### qos dscp-color-policy

Associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map.

**Syntax**

```
dscp-color-policy color-map-profile-name
```

To remove a color policy map profile, use the `no dscp-color-policy color-map-profile-name` command.

**Parameters**

- **color-map-profile-name**
  
Enter the color map profile name. The name can have a maximum of 32 characters.

**Defaults**

None

**Command Modes**

CONFIG-INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(1.0) Introduced on the Z9100-ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Introduced on the S6000-ON.
- 9.5(0.1) Introduced on the Z9500.

**Version 9.5.0.0**

Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

**Usage Information**

If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

**Example**

The following example assigns the color map, `bat-enclave-map`, to interface `gi 1/11`.

Dell(conf)# int gi 1/11
Dell(conf-if-gi-1/11)# qos dscp-color-policy bat-enclave-map

**Related Commands**

- **dscp** — sets the number of specific DSCP values for color map profile to yellow or red.
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.5.0.0 Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Example

Display summary information about a color policy on one or more interfaces.

Dell# show qos dscp-color-policy summary

Interface dscp-color-map
GI 1/10 mapONE
GI 1/11 mapTWO

Display summary information about a color policy on a specific interface.

Dell# show qos dscp-color-policy summary te 1/10/1

Interface dscp-color-map
GI 1/10 mapONE

Displayed detailed color policy information on an interface.

Dell# show qos dscp-color-policy detail te 1/10

Interface GigabitEthernet 1/10
Dscp-color-map mapONE
    yellow 4,7
    red 20,30

Dell#

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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5.0.0</td>
<td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
</tbody>
</table>

**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
Dell#
```
Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking OS supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2) on the platform.

The Dell Networking OS implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, see the Dell Networking OS Configuration Guide.

Topics:
- auto-summary
- clear ip rip
- debug ip rip
- default-information originate
- default-metric
- description
- distance
- distribute-list in
- distribute-list out
- ip poison-reverse
- ip rip receive version
- ip rip send version
- ip split-horizon
- maximum-paths
- neighbor
- network
- offset-list
- output-delay
- passive-interface
- redistribute
- redistribute isis
- redistribute ospf
- router rip
- show config
- show ip rip database
- show running-config rip
- timers basic
- version

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

Syntax

auto-summary
To send sub-prefix routing information, use the `no auto-summary` command.

**Defaults**
- Enabled.

**Command Modes**
- ROUTER RIP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

---

**clear ip rip**

Update all the RIP routes in the Dell Networking OS routing table.

**S3048-ON**

**Syntax**
```
clear ip rip
```

**Command Modes**
- EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
### debug ip rip

Examine RIP routing information for troubleshooting.

**S3048–ON**

**Syntax**

```
debug ip rip [interface | database | events [interface] | trigger]
```

To turn off debugging output, use the `no debug ip rip` command.

**Parameters**

- **interface** (OPTIONAL) Enter the interface type and ID as one of the following:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

- **database** (OPTIONAL) Enter the keyword `database` to display messages when there is a change to the RIP database.

- **events** (OPTIONAL) Enter the keyword `events` to debug only RIP protocol changes.

- **trigger** (OPTIONAL) Enter the keyword `trigger` to debug only RIP trigger extensions.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
default-information originate

Generate a default route for the RIP traffic.

S3048–ON

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


Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.
### 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.

**S3048-ON**

**Syntax**

```
default-metric number
```

To return the default metric to the original values, use the `no default-metric` command.

**Parameters**

- **number**: Specify a number. The range is from 1 to 16. The default is 1.

**Defaults**

1

**Command Modes**

Router RIP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
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.

**S3048-ON**

**Syntax**
```
description {description}
```

To remove the description, use the no description {description} command.

**Parameters**
- **description**
  Enter a description to identify the RIP protocol (80 characters maximum).

**Defaults**
none

**Command Modes**
ROUTER RIP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Introduced on the S3048-ON and S4048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 7.7.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**
- router rip — enters ROUTER mode on the switch.
distance

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights ("administrative distance") are preferred.

S3048-ON

distance weight [ip-address mask [prefix-name]]

To return to the default values, use the no distance weight [ip-address mask] command.

Syntax

Parameters

weight
Enter a number from 1 to 255 for the weight (for prioritization). The default is 120.

ip-address
(Optional) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.

mask
If you enter an IP address, also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x).

prefix-name
(Optional) Enter a configured prefix list name.

Defaults

weight = 120

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- default-metric — assigns one distance metric to all routes learned using the redistribute command.
**distribute-list in**

Configure a filter for incoming routing updates.

**S3048-ON**

**Syntax**

```
distribute-list prefix-list-name in [interface]
```

To delete the filter, use the `no distribute-list prefix-list-name in` command.

**Parameters**

- `prefix-list-name` Enter the name of a configured prefix list.
- `interface` (OPTIONAL) Identifies the interface type slot/port as one of the following:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel` then a number.
  - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.

**Command Modes**

`ROUTER RIP`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(1.0)
- 9.8(0.0P5)
- 9.8(0.0P2)
- 9.7(0.0)
- 9.2(1.0)
- 9.0.2.0
- 8.3.29.0
- 8.3.11.1
- 8.5.1.0
- 8.3.7.0
- 7.8.1.0
- 7.6.1.0
- pre- 6.2.1.1

**Description**

- Introduced on the Z9100-ON.
- Introduced on the S4048-ON.
- Introduced on the S3048-ON.
- Introduced on the S6000-ON.
- Introduced on the S9500.
- Introduced on the S6000.
- Introduced on the S4820T.
- Introduced on the Z9000.
- Added support for 4-port 40G line cards.
- Introduced on the S4810.
- Introduced on the S-Series.
- Introduced on the C-Series.
- Introduced on the E-Series.

**Related Commands**

- `ip prefix-list` — enters PREFIX-LIST mode and configures a prefix list.
**distribute-list out**

Configure a filter for outgoing routing updates.

**S3048-ON**

**Syntax**

```
distribute-list prefix-list-name out [interface | bgp | connected | isis | ospf | static]
```

To delete the filter, use the no distribute-list prefix-list-name out command.

**Parameters**

- `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 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
    - For a Port Channel interface, enter the keywords `port-channel` then a number.
    - For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
- `connected`:
  - (OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
- `isis`:
  - (OPTIONAL) Enter the keyword `isis` to filter only IS-IS routes.
- `ospf`:
  - (OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
- `static`:
  - (OPTIONAL) Enter the keyword `static` to filter manually configured routes.

**Defaults**

Not configured.

**Command Modes**

- ROUTER RIP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5(1.0)</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

S3048-ON

Syntax

ip poison-reverse

To disable poison reverse, use the no ip poison-reverse command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version  Description
9.8(1.0)   Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)   Introduced on the S6000-ON.
9.2(1.0)   Introduced on the Z9500.
9.0.2.0    Introduced on the S6000.
8.3.19.0   Introduced on the S4820T.
8.3.11.1   Introduced on the Z9000.
8.3.7.0    Introduced on the S4810.
7.8.1.0    Introduced on the S-Series.
7.6.1.0    Introduced on the C-Series.
pre- 6.2.1.1 Introduced on the E-Series.

Related Commands

-  ip split-horizon — sets the RIP routing updates to exclude routing prefixes.
ip rip receive version

To receive specific versions of RIP, set the interface. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.

**S3048-ON**

**Syntax**

```
ip rip receive version [1] [2]
```

To return to the default, use the `no ip rip receive version` command.

**Parameters**

- **1** (OPTIONAL) Enter the number 1 for RIP version 1.
- **2** (OPTIONAL) Enter the number 2 for RIP version 2.

**Defaults**

RIPv1 and RIPv2

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.

S3048-ON

Syntax

ip rip send version [1] [2]

To return to the default value, use the no ip rip send version command.

Parameters

1 (OPTIONAL) Enter the number 1 for RIP version 1. The default is RIP version 1.
2 (OPTIONAL) Enter the number 2 for RIP version 2.

Defaults

RIPv1

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To enable the interface to send both version of RIP packets, use the ip rip send version 1 2 command.

Related Commands

- ip rip receive version — sets the RIP version for the interface to receive traffic.
- version — sets the RIP version for the switch software.
**ip split-horizon**

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

### S3048–ON

**Syntax**

```
ip split-horizon
```

To disable split-horizon, use the `no ip split-horizon` command.

**Defaults**

Enabled

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `ip poison-reverse` — sets the prefix for RIP routing updates.

**maximum-paths**

Set RIP to forward packets over multiple paths.

### S3048–ON

**Syntax**

```
maximum-paths number
```

To return to the default values, use the `no maximum-paths` commands.
Parameters

number

Enter the number of paths. The range is from 1 to 16. The default is 4 paths.

Defaults

4

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the S-Series.
7.6.1.0 Introduced on the C-Series.
pre- 6.2.1.1 Introduced on the E-Series.

Usage Information

RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

S3048-ON

Syntax

neighbor ip-address

To delete a neighbor setting, use the no neighbor ip-address command.

Parameters

ip-address

Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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.

### S3048–ON

**Syntax**

```
network ip-address
```

To disable RIP for a network, use the `no network ip-address` command.

**Parameters**

- `ip-address` Specify an IP network address in dotted decimal format. You cannot specify a subnet.

**Defaults**

No RIP network is configured.

**Command Modes**

ROUTER RIP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.
Version | Description
--- | ---
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.6.1.0 | Introduced on the C-Series.
pre- 6.2.1.1 | Introduced on the E-Series.

Usage Information
You can enable an unlimited number of RIP networks.
RIP operates over interfaces configured with any address the network command specifies.

offset-list

Specify a number to add to the incoming or outgoing route metrics learned using RIP.

S3048–ON

Syntax
offset-list prefix-list-name {in | out} offset [interface]

To delete an offset list, use the no offset-list prefix-list-name {in | out} offset [interface] command.

Parameters

- **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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a VLAN, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
ROUTER RIP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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.

**S3048-ON**

**Syntax**

```plaintext
output-delay delay
```

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

**Parameters**

- `delay` Specify a number of milliseconds as the delay interval. The range is from 8 to 50.

**Defaults**

Not configured.

**Command Modes**

- ROUTER RIP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
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 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

`ROUTER RIP`

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.5.1.0 | Added support for 4-port 40G line cards on the E-Series.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the C-Series.
7.6.1.0 | Introduced on the E-Series.
pre-6.2.1.1 | Introduced on the E-Series.

**Usage Information**
Although the passive interface does not send or receive routing updates, the network on that interface still includes in RIP updates sent using other interfaces.

**Related Commands**
- `neighbor` — enables RIP for a specified network.
- `network` — defines a neighbor.

**redistribute**
Redistribute information from other routing instances.

**S3048–ON**

**Syntax**
```
redistribute {connected | static}
```
To disable redistribution, use the no redistribute {connected | static} command.

**Parameters**
- `connected` Enter the keyword connected to specify that information from active routes on interfaces is redistributed.
- `static` Enter the keyword static to specify that information from static routes is redistributed.

**Defaults**
Not configured.

**Command Modes**
- ROUTER RIP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
**Version** | **Description**
---|---
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the S-Series.
7.6.1.0 | Introduced on the C-Series.
pre-6.2.1.1 | Introduced on the E-Series.

**Usage Information**
To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

**Related Commands**
- `default-information originate` — generates a default route for RIP traffic.

## redistribute isis

Redistribute routing information from an IS-IS instance.

### S3048–ON

**Syntax**
```
redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]
```

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]` command.

**Parameters**
- **tag** (OPTIONAL) Enter the name of the IS-IS routing process.
- **level-1** (OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
- **level-1-2** (OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
- **level-2** (OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
- **metric metric-value** (OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 0 to 16.
- **route-map map-name** (OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

**Defaults**
Not configured.

**Command Modes**
- ROUTER RIP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version | Description
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.2(1.0) | Introduced on the Z9500.
redistribute ospf

Redistribute routing information from an OSPF process.

S3048-ON

Syntax
redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name]

To disable redistribution, use the no redistribute ospf process-id [match external {1 | 2} | match internal | metric metric-value] [route-map map-name] command.

Parameters
- **process-id**: Enter a number that corresponds to the OSPF process ID to redistribute. The range is from 1 to 65355.
- **match external {1 | 2}**: (OPTIONAL) Enter the keywords match external then the numbers 1 or 2 to indicated that external 1 routes or external 2 routes should be redistributed.
- **match internal**: (OPTIONAL) Enter the keywords match internal to indicate that internal routes should be redistributed.
- **metric metric-value**: (OPTIONAL) Enter the keyword metric then a number as the metric value. The range is from 0 to 16.
- **route-map map-name**: (OPTIONAL) Enter the keywords route-map then the name of a configured route map.

Defaults
Not configured.

Command Modes
- ROUTER RIP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
router rip

To configure and enable RIP, enter ROUTER RIP mode.

S3048-ON

Syntax

```
router rip
```

To disable RIP, use the `no router rip` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6(1)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To enable RIP, assign a network address using the `network` command.

Example

```
Dell(conf)# router rip
Dell(conf-router_rip)#
```

Related Commands

- `network` — enables RIP.
• exit — returns to CONFIGURATION mode.

show config

Display the changes you made to the RIP configuration. The default values are not shown.

S3048–ON

Syntax

show config

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Example

Dell(conf-router_rip)# show config
!
router rip
    network 172.31.0.0
    passive-interface GigabitEthernet 1/1
Dell(conf-router_rip)#

show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

S3048–ON

Syntax

show ip rip database [ip-address mask]
Parameters

- **ip-address** (OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, also enter a mask for that IP address.

- **mask** (OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre- 6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The following describes the **show ip rip database** command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of routes in RIP database</td>
<td>Displays the number of RIP routes stored in the RIP database.</td>
</tr>
<tr>
<td>100.10.10.0/24</td>
<td>Lists the routes directly connected.</td>
</tr>
<tr>
<td>150.100.0.0</td>
<td>Lists the routes learned through redistribution.</td>
</tr>
<tr>
<td>209.16.0.24</td>
<td>Lists the routes and the sources advertising those routes.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
    [50/1] via 192.14.1.3, 00:00:12, GigabitEthernet 1/15
204.250.54.0/24     auto-summary
203.250.49.0/24
    [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 1/14
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
```
show running-config rip

Display the current RIP configuration.

**S3048-ON**

**Syntax**

```
show running-config rip
```

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show running-config rip
!
router rip
  distribute-list Test1 in
  distribute-list Test21 out
  network 10.0.0.0
  passive-interface GigabitEthernet 2/1
  neighbor 20.20.20.20
  redistribute ospf 999
  version 2
Dell#
```
timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times, and flush time.

S3048-ON

Syntax

```
timers basic update invalid holddown flush
```

To return to the default settings, use the `no timers basic` command.

Parameters

- **update**
  - Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is from zero (0) to 4294967295. The default is `30 seconds`.

- **invalid**
  - Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is `180 seconds`.

- **holddown**
  - Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is `180 seconds`.

- **flush**
  - Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is from zero (0) to 4294967295. The default is `240 seconds`.

Defaults

- `update = 30 seconds`
- `invalid = 180 seconds`
- `holddown = 180 seconds`
- `flush = 240 seconds`

Command Modes

```
ROUTER RIP
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.

**S3048-ON**

**Syntax**

`version {1 | 2}`

To return to the default version setting, use the `no version` command.

**Parameters**

- **1**
  - Enter the keyword `1` to specify RIP version 1.
- **2**
  - Enter the keyword `2` to specify RIP version 2.

**Defaults**

The Dell Networking OS sends RIPv1 and receives RIPv1 and RIPv2.

**Command Modes**

`ROUTER RIP`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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 OS remote monitoring (RMON) is implemented on the S3048–ON platform. Dell Networking OS RMON is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection. Dell Networking OS RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, RFC-3434, and RFC-4502:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819
- User History; RFC-4502
- Probe Configuration (Capabilities, SoftwareRev, HardwareRev, DateTime and ResetControl); RFC-4502

Dell Networking OS RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

**NOTE:** Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

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.

S3048–ON

Syntax

```
 rmon alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]
```

To disable the alarm, use the no rmon alarm number command.

Parameters

- **number**: Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
- **variable**: Enter the MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3. The object type must be a 32-bit integer.
- **interval**: Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
- **delta**: Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
- **absolute**: Enter the keyword absolute to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
- **rising-threshold**: Enter the keywords rising-threshold then the value (32 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
- **falling-threshold**: Enter the keywords falling-threshold then the value (32 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
- **owner string**: (OPTIONAL) Enter the keyword owner then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults

owner

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

**S3048–ON**

**Syntax**

```
(rmon collection history {controlEntry integer} [owner name] [buckets number] [interval seconds])
```

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry integer}` command.

**Parameters**

- **controlEntry integer**: Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON history table.
- **owner name**: (OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.
- **buckets number**: (OPTIONAL) Enter the keyword `buckets` then the number of buckets for the RMON collection history group of statistics. The bucket range is from 1 to 1000. The default is 50.
- **interval seconds**: (OPTIONAL) Enter the keyword `interval` then the number of seconds in each polling cycle. The range is from 5 to 3600 seconds. The default is 1800 seconds.

**Defaults**

none

**Command Modes**

CONFIGURATION INTERFACE (config-if)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
**rmon collection statistics**

Enable RMON MIB statistics collection on an interface.

**S3048–ON**

**Syntax**

```
rmon collection statistics {controlEntry integer} [owner name]
```

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry integer}` command.

**Parameters**

- **controlEntry integer**
  
  Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON statistic table.

- **owner name**
  
  (OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.

**Defaults**

`none`

**Command Modes**

`CONFIGURATION INTERFACE (config-if)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

rmon event

Add an event in the RMON event table.

S3048–ON

Syntax

rmon event number [log] [trap community] [description string]

To disable RMON on an interface, use the no rmon event number command.

Parameters

number

Assign an event number in integer format. The range is from 1 to 65535. You must ensure that the value you enter is unique in the RMON event table.

log

(OPTIONAL) Enter the keyword log to generate an RMON event log. This option sets the eventType to either log or log-and-snmptrap in the RMON event table. The default is None.

trap community

(OPTIONAL) Enter the keyword trap followed by the SNMP community string to generate SNMP traps for an RMON event entry. This option sets the eventType to either snmptrap or log-and-snmptrap in the RMON event table. In addition to the SNMP traps, this option also generates a syslog.

description string

(OPTIONAL) Enter the keyword description then a string describing the event.

owner name

(OPTIONAL) Enter the keyword owner then the name of the owner of this event.

Defaults

As noted in the Parameters section.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version     Description

9.8(1.0)     Introduced on the Z9100-ON.
9.8(0.0P5)   Introduced on the S4048-ON.
9.8(0.0P2)   Introduced on the S3048-ON.
9.7(0.0)     Introduced on the S6000-ON.
9.2(1.0)     Introduced on the Z9500.
9.0.2.0      Introduced on the S6000.
8.3(19.0)    Introduced on the S4820T.
8.3(11.1)    Introduced on the Z9000.
rmon hc-alarm

Set an alarm on any MIB object.

S3048-ON

Syntax

rmon hc-alarm number variable interval {delta | absolute} rising-threshold value event-number falling-threshold value event-number [owner string]

To disable the alarm, use the no rmon hc-alarm number command.

Parameters

- **number**: Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
- **variable**: The MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3 The object type must be a 64-bit integer.
- **interval**: Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
- **delta**: Enter the keyword delta to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
- **absolute**: Enter the keyword absolute to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
- **rising-threshold value event-number**: Enter the keywords rising-threshold then the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
- **falling-threshold value event-number**: Enter the keywords falling-threshold then the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
- **owner string**: (OPTIONAL) Enter the keyword owner then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults

- owner

Command Modes

- CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**show rmon**

Display the RMON running status including the memory usage.

### S3048-ON

**Syntax**

```
show rmon
```

**Defaults**

none

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
show rmon alarms

Display the contents of the RMON alarm table.

S3048–ON

Syntax

show rmon alarms [index] [brief]

Parameters

- **index**: (OPTIONAL) Enter the table index number to display just that entry.
- **brief**: (OPTIONAL) Enter the keyword **brief** to display the RMON alarm table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
show rmon events

Display the contents of the RMON event table.

S3048–ON

**Syntax**
```
show rmon events [index] [brief]
```

**Parameters**
- `index` (OPTIONAL) Enter the table index number to display just that entry.
- `brief` (OPTIONAL) Enter the keyword `brief` to display the RMON event table in an easy-to-read format.

**Defaults**
none

**Command Modes**
EXEC

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
6.1.1.0 | Introduced on the E-Series.

**Example (Index)**

Dell(conf)# rmon event 111
Dell(conf)# rmon event 112 log
Dell(conf)# rmon event 113 trap private
Dell(conf)# rmon event 114 log trap public
Dell(conf)# do show rmon events

RMON event entry 111
  description:
  event type: none.
  event community:
  event last time sent: none
  event owner:
  event status: OK

RMON event entry 112
  description:
  event type: LOG.
  event community:
  event last time sent: none
  event owner:
  event status: OK

RMON event entry 113
  description:
  event type: SNMP TRAP.
  event community: private
  event last time sent: none
  event owner:
  event status: OK

RMON event entry 114
  description:
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner:
  event status: OK

**Example (Brief)**

Dell# show rmon event brief
index  description
-------  ---------------------------------------
  1      1
  2      2
  3      3
  4      4
  5      5
  6      6
  7      7
show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

S3048–ON

Syntax

show rmon hc-alarm [index] [brief]

Parameters

index

(Optional) Enter the table index number to display just that entry.

brief

(Optional) Enter the keyword brief to display the RMON High-Capacity alarm table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
show rmon history

Display the contents of the RMON Ethernet history table.

**S3048-ON**

**Syntax**

```
show rmon history [index] [brief]
```

**Parameters**

- `index`  
  (OPTIONAL) Enter the table index number to display just that entry.

- `brief`  
  (OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet history table in an easy-to-read format

**Defaults**

none

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
show rmon log

Display the contents of the RMON log table.

**S3048-ON**

**Syntax**

```
show rmon log [index] [brief]
```

**Parameters**

- **index**  
  (OPTIONAL) Enter the table index number to display just that entry.
- **brief**  
  (OPTIONAL) Enter the keyword `brief` to display the RMON log table in an easy-to-read format.

**Defaults**

none

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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
eventId     description
-----------  ---------------
  2           2
  4           4
Dell#

**show rmon statistics**

Display the contents of RMON Ethernet statistics table.

**S3048-ON**

**Syntax**

```
show rmon statistics [index] [brief]
```

**Parameters**

- **index**
  - (OPTIONAL) Enter the table index number to display just that entry.
- **brief**
  - (OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet statistics table in an easy-to-read format.

**Defaults**

`none`

**Command Modes**

`EXEC`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example (Index)**

```
Dell# show rmon statistics 6001
RMON statistics entry 6001
    interface: ifIndex.100974631 GigabitEthernet 2/1
    packets dropped: 0
    bytes received: 0
    packets received: 0
    broadcast packets: 0
    multicast packets: 0
    CRC error: 0
    under-size packets: 0
    over-size packets: 0
    fragment errors: 0
    jabber errors: 0
    collision: 0
    64bytes packets: 0
    65-127 bytes packets: 0
    128-255 bytes packets: 0
    256-511 bytes packets: 0
    512-1023 bytes packets: 0
    1024-1518 bytes packets: 0
    owner: 1
    status: OK
    <high-capacity data>
    HC packets received overflow: 0
    HC packets received: 0
    HC bytes received overflow: 0
    HC bytes received: 0
    HC 64bytes packets overflow: 0
    HC 64bytes packets: 0
    HC 65-127 bytes packets overflow: 0
    HC 65-127 bytes packets: 0
    HC 128-255 bytes packets overflow: 0
    HC 128-255 bytes packets: 0
    HC 256-511 bytes packets overflow: 0
    HC 256-511 bytes packets: 0
    HC 512-1023 bytes packets overflow: 0
    HC 512-1023 bytes packets: 0
    HC 1024-1518 bytes packets overflow: 0
    HC 1024-1518 bytes packets: 0
Dell#
```

**Example (Brief)**

```
Dell# show rmon statistics br
index   ifIndex   interface
----------------------------------------
```

Remote Monitoring (RMON)
<table>
<thead>
<tr>
<th>Device</th>
<th>Port Number</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>6001</td>
<td>6002</td>
<td>GigabitEthernet 2/2</td>
</tr>
<tr>
<td>6003</td>
<td>6004</td>
<td>GigabitEthernet 2/1</td>
</tr>
<tr>
<td>9001</td>
<td>9002</td>
<td>GigabitEthernet 3/2</td>
</tr>
<tr>
<td>9003</td>
<td>9004</td>
<td>GigabitEthernet 3/1</td>
</tr>
</tbody>
</table>

Dell# Remote Monitoring (RMON) 1273
Rapid Spanning Tree Protocol (RSTP)

The Dell Networking 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.

Dell Networking OS supports RSTP.

Topics:
- bridge-priority
- debug spanning-tree rstp
- description
- disable
- forward-delay
- hello-time
- max-age
- protocol spanning-tree rstp
- show config
- show spanning-tree rstp
- spanning-tree rstp
- tc-flush-standard

bridge-priority

Set the bridge priority for RSTP.

Syntax  

```
bridge-priority priority-value
```

To return to the default value, use the no bridge-priority command.

Parameters

- **priority-value**
  
Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is 32768.

Defaults

32768

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.
### debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

**Syntax**

```
debug spanning-tree rstp [all | bpdu interface {in | out} | events]
```

To disable debugging, use the `no debug spanning-tree rstp` command.

**Parameters**

- **all** (OPTIONAL) Enter the keyword all to debug all spanning tree operations.
- **bpdu interface {in | out}** (OPTIONAL) Enter the keyword bpdu to debug the bridge protocol data units. Enter the keyword interface along with the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port-channel interface, enter the keywords port-channel then the port-channel ID.

  Optionally, enter an in or out parameter with the optional interface:
  - For Receive, enter in.
  - For Transmit, enter out.

- **events** (OPTIONAL) Enter the keyword events to debug RSTP events.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
**description**

Enter a description of the rapid spanning tree.

**Syntax**

```plaintext
description {description}
```

To remove the description, use the `no description {description}` command.

**Parameters**

- `description` Enter a description to identify the rapid spanning tree (80 characters maximum).

**Defaults**

none

**Command Modes**

SPANNING TREE (The prompt is "config-rstp.")

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
disable

Disable RSTP globally on the system.

Syntax
disable

To enable Rapid Spanning Tree Protocol, use the no disable command.

Defaults
RSTP is disabled.

Command Modes
CONFIGURATION RSTP (conf-rstp)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Related Commands
- protocol spanning-tree rstp — enters SPANNING TREE mode on the switch.

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Syntax
forward-delay seconds

To return to the default setting, use the no forward-delay command.
Parameters

seconds

Enter the number of seconds that Dell Networking OS waits before transitioning RSTP to the forwarding state. The range is from 4 to 30. The default is 15 seconds.

Defaults

15 seconds

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3(19.0) Introduced on the S4820T.
8.3(11.1) Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Related Commands

• hello-time — changes the time interval between BPDUs.
• max-age — changes the wait time before RSTP refreshes the protocol configuration information.

hello-time

Set the time interval between the generation of the RSTP bridge protocol data units (BPDUs).

Syntax

hello-time [milli-second] seconds

To return to the default value, use the no hello-time command.

Parameters

seconds

Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10 seconds. The default is 2 seconds.

milli-second

Enter the keywords milli-second to configure a hello time on the order of milliseconds. The range is from 50 to 950 milliseconds

Defaults

2 seconds

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

1278 | Rapid Spanning Tree Protocol (RSTP)
**Usage Information**

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals \((x/1000)\times256\).

When you configure millisecond hellos, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

**Related Commands**

- `forward-delay` — changes the wait time before RSTP transitions to the Forwarding state.
- `max-age` — changes the wait time before RSTP refreshes the protocol configuration information.

**max-age**

To maintain configuration information before refreshing that information, set the time interval for the RSTP bridge.

**Syntax**

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

**Parameters**

- `max-age` Enter a number of seconds the Dell Networking OS waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is 20 seconds.

**Defaults**

20 seconds

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
Version  | Description
--- | ---
9.8(0.0P5)  | Introduced on the S4048-ON.
9.8(0.0P2)  | Introduced on the S3048-ON.
9.7(0.0)  | Introduced on the S6000-ON.
9.2(1.0)  | Introduced on the Z9500.
9.0.2.0  | Introduced on the S6000.
8.3.19.0  | Introduced on the S4820T.
8.3.11.1  | Introduced on the Z9000.
8.3.7.0  | Introduced on the S4810.
7.6.1.0  | Introduced on the S-Series.
7.5.1.0  | Introduced on the C-Series.
6.2.1.1  |Introduced on the E-Series.

Related Commands
- forward-delay — changes the wait time before RSTP transitions to the Forwarding state.
- hello-time — changes the time interval between BPDUs.

**protocol spanning-tree rstp**

To configure RSTP, enter RSTP mode.

**Syntax**

```plaintext
protocol spanning-tree rstp
```

To exit RSTP mode, use the `exit` command.

**Defaults**

Not configured

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**  | **Description**
--- | ---
9.8(1.0)  | Introduced on the Z9100-ON.
9.8(0.0P5)  | Introduced on the S4048-ON.
9.8(0.0P2)  | Introduced on the S3048-ON.
9.7(0.0)  | Introduced on the S6000-ON.
9.2(1.0)  | Introduced on the Z9500.
9.0.2.0  | Introduced on the S6000.
8.3.19.0  | Introduced on the S4820T.
8.3.11.1  | Introduced on the Z9000.
8.3.7.0  | Introduced on the S4810.
7.6.1.0  | Introduced on the S-Series.
7.5.1.0  | Introduced on the C-Series.
Version | Description
------- | -------
6.2.1.1  | Introduced on the E-Series.

Usage Information

RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the no disable command from RSTP mode.

Example

Dell(conf)# protocol spanning-tree rstp
Dell(config-rstp)# no disable

Related Commands

- disable — disables RSTP globally on the system.

**show config**

View the current configuration for the mode. Only non-default values are displayed.

**Syntax**

```
show config
```

**Command Modes**

CONFIGURATION RSTP (conf-rstp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf-rstp)# show config

! protocol spanning-tree rstp
  no disable
  bridge-priority 16384
```

**show spanning-tree rstp**

Display the RSTP configuration.

**Syntax**

```
show spanning-tree rstp [brief] [guard]
```
Parameters

brief  (OPTIONAL) Enter the keyword brief to view a synopsis of the RSTP configuration information.

guard  (OPTIONAL) Enter the keyword guard to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version   Description
---------   -----------------------------------------
9.8(1.0)   Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)   Introduced on the S6000-ON.
9.2(1.0)   Introduced on the Z9500.
9.0.2.0    Introduced on the S6000.
8.3(19.0)  Introduced on the S4820T.
8.3(11.1)  Introduced on the Z9000.
8.4.2.1    Added support for the optional guard keyword on the C-Series, S-Series, and E-Series.
8.3.7.0    Introduced on the S4810.
7.6.1.0    Introduced on the S-Series.
7.5.1.0    Introduced on the C-Series.
6.4.1.0    Expanded to display the port error disable state (EDS) caused by loopback BPDU inconsistency.
6.2.1.1    Introduced on the E-Series.

Usage Information

The following describes the show spanning-tree rstp guard command shown in the following example.

Field   Description
---------   -----------------------------------------
Interface Name   RSTP interface.
Instance   RSTP instance.
Sts   Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), disabled (DIS), or shut down (EDS Shut).
Guard Type   Types of STP guard configured (Root, Loop, or BPDU guard)

Example (Brief)

```
Dell# show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15
Interface   Designated
Name   PortID Prio Cost Sts Cost Bridge ID PortID
-------- ------- --- ------- ------------------ -------- --------
```
Example (EDS, LBK)

NOTE: "LBK_INC" (bold) means Loopback BPDU Inconsistency.

Dell# show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Example (Guard)

Dell# show spanning-tree rstp guard
Interface
Name Instance Sts Guard type
--------- ------- ---------------
Gi 0/1 0 INCON(Root) Rootguard
Gi 0/2 0 FWD Loopguard
Gi 0/3 0 BLK Bpduguard

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

Syntax

spanning-tree rstp {cost port-cost | edge-port [bpduguard [shutdown-on-violation]]} | priority priority | {loopguard | rootguard}
Parameters

- **cost port-cost**: Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are:
  - 100 Mb/s Ethernet interface = 200000
  - 1-Gigabit Ethernet interface = 20000
  - 10-Gigabit Ethernet interface = 2000
  - Port Channel interface with one 100 Mb/s Ethernet = 200000
  - Port Channel interface with one 1 Gigabit Ethernet = 20000
  - Port Channel interface with one 10 Gigabit Ethernet = 2000
  - Port Channel with two 1 Gigabit Ethernet = 18000
  - Port Channel with two 10 Gigabit Ethernet = 1800
  - Port Channel with two 100 Mbps Ethernet = 180000

- **edge-port**: Enter the keywords `edge-port` to configure the interface as a rapid spanning tree edge port.

- **bpduguard**: (OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails.

  Enter the keyword `bpduguard` to disable the port when it receives a BPDU.

- **shutdown-on-violation**: (OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

- **priority priority**: Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is 128.

- **loopguard**: Enter the keyword `loopguard` to enable loop guard on an RSTP port or port-channel interface.

- **rootguard**: Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

**Defaults**
Not configured.

**Command Modes**

- INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Added support for the optional <code>guard</code> keyword on the C-Series, S-Series, and E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1.0</td>
<td>Introduced the hardware shutdown-on-violation options.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Added the optional bridge port data unit (BPDU) guard.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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, BPDPUs 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

```bash
Dell(conf)# interface gigabitethernet 4/1
Dell(conf-if-gi-4/0)# spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)# show config
!
interface GigabitEthernet 4/1
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

### tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

**Syntax**

```
tc-flush-standard
```

To disable, use the no tc-flush-standard command.

**Defaults**

Disabled

**Command Modes**

CONFIGURATION (conf-rstp)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, Dell Networking OS implements an optimized flush mechanism for RSTP. This implementation helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this knob command to enable flushing MAC addresses after receiving every topology change notification.
Software-Defined Networking (SDN)

The Dell Networking OS supports software-defined networking (SDN). For more information, see the SDN Deployment Guide.
The commands in this chapter are available on Dell Networking OS.
For configuration details, see the Security section in the Dell Networking OS Configuration Guide.

NOTE: Dell Networking OS implements LEAP with MSCHAP v2 supplicant.

Topics:
- AAA Accounting Commands
- Authorization and Privilege Commands
- Obscure Password Commands
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- Port Authentication (802.1X) Commands
- SSH and SCP Commands
- Secure DHCP Commands
- Role-Based Access Control 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 | role role-name} {name | default}{start-stop | wait-start | stop-only} {tacacs+}

Parameters
- system: Enter the keyword system to send accounting information of any other AAA configuration.

To disable AAA Accounting, use the no aaa accounting {system | exec | command level} {name | default}{start-stop | wait-start | stop-only} {tacacs+} command.
exec

Enter the keyword exec to send accounting information when a user has logged in to EXEC mode.

commands (level | role role-name)

Enter the keyword command then a privilege level for accounting of commands executed at that privilege level or enter the keyword role then the role name for accounting of commands executed by a user with that user role.

name | default

Enter one of the following:

- For name, enter a user-defined name of a list of accounting methods.
- For default, the default accounting methods used.

start-stop

Enter the keywords start-stop to send a “start accounting” notice at the beginning of the requested event and a “stop accounting” notice at the end of the event.

wait-start

Enter the keywords wait-start to ensure that the TACACS+ security server acknowledges the start notice before granting the user’s process request.

stop-only

Enter the keywords stop-only to instruct the TACACS+ security server to send a “stop record accounting” notice at the end of the requested user process.

tacacs+

Enter the keyword tacacs+ to use TACACS+ data for accounting. The Dell Networking OS currently only supports TACACS+ accounting.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0)     Introduced on the Z9100-ON.
9.8(0.0P5)   Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)     Introduced on the S6000--ON.
9.5(0.0)     Added support for roles on the Z9000, S6000, S4820T, S4810, and M40X.
9.2(1.0)     Introduced on the Z9500.
9.0.2.0      Introduced on the S6000.
8.3.19.0     Introduced on the S4820T.
8.3.11.1     Introduced on the Z9000.
8.3.7.0      Introduced on the S4810.
7.6.1.0      Introduced on the S-Series.
7.5.1.0      Introduced on the C-Series.
6.3.1.0      Introduced on the E-Series.

Usage Information

In the example above, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1 for example, use the aaa accounting command 1 command.
Example

Dell(conf)# aaa accounting exec default start-stop tacacs+
Dell(conf)# aaa accounting command 15 default start-stop tacacs+
Dell(conf)# aaa accounting command role secaadmin default start-stop tacacs+

Related Commands

- enable password — changes the password for the enable command.
- login authentication — enables AAA login authentication on the terminal lines.
- password — creates a password.
- tacacs-server host — specifies a TACACS+ server host.

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 keyword role and then the role name for accounting of commands executed by a user with that user role.

method-list

Enter a method list that you defined using the aaa accounting exec or aaa accounting commands.

Defaults

none

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
aaa accounting suppress

Prevent the generation of accounting records of users with the user name value of NULL.

Syntax

```
aaa accounting suppress null-username
```

To permit accounting records to users with user name value of NULL, use the `no aaa accounting suppress null-username` command.

Defaults

Accounting records are recorded for all users.

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4280T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
```

Usage Information

Dell Networking OS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login method-list none` command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the `aaa accounting suppress` command.

aaa radius group

Configure the RADIUS server group that is used for Authentication, Authorization and Accounting.

Syntax

```
aaa radius group group-name
```

Usage Information

Dell Networking OS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login method-list none` command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the `aaa accounting suppress` command.
To remove the RADIUS group configuration, use the `no aaa radius group group-name` command.

**Parameters**

- **group-name**
  
  Enter the name of the RADIUS server group.

**Defaults**

- none

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can use this command to configure the group of Radius servers used for Authentication, Authorization, and Accounting purposes.

If the RADIUS group is not configured for Authentication, Authorization, and Accounting, then globally configured Radius servers are used for the purposes.

When the RADIUS group is removed, the AAA configuration is also removed.

**Example**

```
Dell(conf)# radius-server group group1
Dell(conf-radius-group)# radius-server host 1.1.1.1 key secret
Dell(conf-radius-group)# radius-server host 2.2.2.2 key secret
Dell(conf-radius-group)# radius-server vrf vrf1 source-interface gigabitethernet 1/36
Dell(conf)# exit
Dell(conf)# aaa radius group group1
```

**show accounting**

Display the active accounting sessions for each online user.

**Syntax**

```
show accounting
```

**Defaults**

- none

**Command Modes**

- EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Added support for roles on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command steps through all active sessions and then displays the accounting records for the active account functions.

**Example**

```
Dell# show accounting
Active accounted actions on tty2, User admin Priv 1 Role
Task ID 2, EXEC Accounting record, 00:02:03 Elapsed, service=shell
Active accounted actions on tty3, User ad Priv 15 Role
    Task ID 7, EXEC Accounting record, 00:01:22 Elapsed, service=shell
Active accounted actions on tty4, User ad Priv 15 Role
    Task ID 11, EXEC Accounting record, 00:00:35 Elapsed, service=shell
Active accounted actions on tty5, User ad1 Priv 1 Role sysadmin
    Task ID 16, EXEC Accounting record, 00:00:04 Elapsed, service=shell
Dell#
```

**Related Commands**

- `aaa accounting` — enables AAA Accounting and creates a record for monitoring the accounting function.

**Authorization and Privilege Commands**

To set command line authorization and privilege levels, use the following commands.

**authorization**

Apply an authorization method list to terminal lines.

**Syntax**

```
authorization {exec | commands {level | role role-name}} method-list
```

**Parameters**

- `exec`  
  Enter the keyword `exec` to apply an EXEC level authorization method list.

- `commands {level | role role-name}`  
  Enter the keyword `commands` followed by either a privilege level for accounting of commands executed at that privilege level, or enter the keyword `role` then the role name for authorization of commands executed by a user with that user role.
method-list

Enter a method list that you defined using the aaa accounting exec or aaa accounting commands.

Defaults
none

Command Modes
LINE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for roles on the Z9000, S6000, S4820T, S4810, and M4x.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands
• aaa authorization commands — sets the parameters that restrict (or permit) a user’s access to EXEC and CONFIGURATION level commands.
• aaa authorization exec — sets the parameters that restrict (or permit) a user’s access to EXEC level commands.

aaa authorization commands

Set parameters that restrict (or permit) a user’s access to EXEC and CONFIGURATION level commands.

Syntax
aaa authorization commands {level | role role-name}{name|default} {local | tacacs+ | none}
Undo a configuration with the no aaa authorization commands {level | role role-name}{name|default} {local | tacacs+ | none} command.

Parameters
commands level
Enter the keyword commands then the command privilege level for command level authorization.
role role-name
Enter the keyword role then the role name.
name
Define a name for the list of authorization methods.
default
Define the default list of authorization methods.
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

Usage Information

Certain TACACS+ servers do not authenticate the device if you use the aaa authorization commands
level default local tacacs+ command. To resolve the issue, use the aaa authorization commands level default tacacs+ local command.

aaa authorization config-commands
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Added support for RADIUS.</td>
</tr>
</tbody>
</table>

**privilege level (CONFIGURATION mode)**

Change the access or privilege level of one or more commands.

**Syntax**

```
privilege mode {level level command | reset command}
```

To delete access to a level and command, use the no privilege mode level level command command.

**Parameters**

- **mode**
  - Enter one of the following keywords as the mode for which you are controlling access:
    - configure for CONFIGURATION mode
    - exec for EXEC mode
    - interface for INTERFACE modes
    - line for LINE mode
    - route-map for ROUTE-MAP mode
    - router for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes

- **level level**
  - Enter the keyword level then a number for the access level. The range is from 0 to 15.
  - Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.

- **reset**
  - Enter the keyword reset to return the security level to the default setting.

- **command**
  - Enter the command’s keywords to assign the command to a certain access level. You can enter one or all of the keywords.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
### privileged 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Obscure Password Commands

To enable the obscure password, use the following commands.

**service obscure-passwords**

Enable the obscuring of passwords and keys.

**Syntax**

```
service obscure-passwords
```

Enable the obscuring of passwords and keys, including RADIUS, TACACS+ keys, router authentication strings, VRRP authentication, use the `service obscure-passwords` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, Z9000, Z9500, MXL</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, the `service password-encryption` command stores encrypted passwords. For greater security, you can also use the `service obscure-passwords` command to prevent a user from reading the passwords and keys, including RADIUS, TACACS+ keys, router authentication strings, VRRP authentication by obscuring this information. Passwords and keys are stored encrypted in the configuration file and by default are displayed in the encrypted form when the configuration is displayed. Enabling the `service obscure-passwords` command displays asterisks instead of the encrypted passwords and keys. This command prevents a user from reading these passwords and keys by obscuring this information with asterisks.

Password obscuring masks the password and keys for display only but does not change the contents of the file. The string of asterisks is the same length as the encrypted string for that line of configuration. To verify that you have successfully obscured passwords and keys, use the `show running-config command` or `show startup-config command`.

If you are using role-based access control (RBAC), only the system administrator and security administrator roles can enable the `service obscure-password` command.

**Related Commands**

- `show running-config` — Display the current configuration and display changes from the default values.
- `service password-encryption` — Encrypts all passwords configured in the system.
Authentication and Password Commands

To manage access to the system, use the following the commands.

**aaa authentication enable**

Configure AAA Authentication method lists for user access to EXEC privilege mode (the “Enable” access).

**Syntax**

```
aaa authentication enable {default | method-list-name} method [... method2]
```

To return to the default setting, use the

```
no aaa authentication enable {default | method-list-name} method [... method2]
```

**Parameters**

- **default**
  - Enter the keyword default then the authentication methods to use as the default sequence of methods for the Enable login. The default is default enable.
- **method-list-name**
  - Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.
- **method**
  - Enter one of the following methods:
    - **enable**
      - Use the password the enable password command defines in CONFIGURATION mode.
    - **line**
      - Use the password the password command defines in LINE mode.
    - **none**
      - No authentication.
    - **radius**
      - Use the RADIUS servers configured with the radius-server host command.
    - **tacacs+**
      - Use the TACACS+ server(s) configured with the tacacs-server host command.

- **... method2**
  - (OPTIONAL) In the event of a “no response” from the first method, Dell Networking OS applies the next configured method.

**Defaults**

Use the enable password.

**Command Modes**

- **CONFIGURATION**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

By default, the Enable password is used. If you configure `aaa authentication enable default`, Dell Networking OS uses the methods defined for Enable access instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

**Related Commands**

- `enable password` — changes the password for the enable command.
- `login authentication` — enables AAA login authentication on the terminal lines.
- `password` — creates a password.
- `radius-server host` — specifies a RADIUS server host.
- `tacacs-server host` — specifies a TACACS+ server host.

## aaa authentication login

Configure AAA Authentication method lists for user access to EXEC mode (Enable log-in).

**Syntax**

```plaintext
aaa authentication login {method-list-name | default} method [... method4]
```

To return to the default setting, use the `no aaa authentication login {method-list-name | default} command.`

**Parameters**

- `method-list-name`  
  Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
- `default`  
  Enter the keyword default to specify that the method list specified is the default method for all terminal lines.
- `method`  
  Enter one of the following methods:
  - `enable`: use the password the enable password command defines in CONFIGURATION mode. Not available if role-only is in use.
  - `line`: use the password the password command defines in LINE mode. Not available if role-only is in use.
  - `local`: use the password for the userid contained in the local password database.
  - `none`: no authentication. Not available if role-only is in use.
  - `radius`: use the RADIUS servers configured with the radius-server host command.
• tacacs+: use the TACACS+ servers configured with the tacacs-server host command.

... method4

(Optional) Enter up to four additional methods. In the event of a “no response” from the first method, the system applies the next configured method (up to four configured methods).

Defaults
Not configured (that is, no authentication is performed).

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000--ON.
9.5(0.1) Added support for roles Z9500.
9.5(0.0) Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.2.1.0 Introduced on the E-Series.

Usage Information
By default, the locally configured username password is used. If you configure aaa authentication login default, Dell Networking OS uses the methods this command defines for login instead.

Methods configured with the aaa authentication login command are evaluated in the order they are configured. If users encounter an error with the first method listed, Dell Networking OS applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user’s name is not listed in the local database, the next method is applied. If the correct user name/password combination is not entered, the user is not allowed access to the switch.

NOTE: If authentication fails using the primary method, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

After configuring the aaa authentication login command, configure the login authentication command to enable the authentication scheme on terminal lines.

Connections to the SSH server work with the following login mechanisms: local, radius, and tacacs.
Related Commands

- `login authentication` — enables AAA login authentication on the terminal lines.
- `password` — creates a password.
- `radius-server host` — specifies a RADIUS server host.
- `tacacs-server host` — specifies a TACACS+ server host.

**access-class**

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

**Syntax**

```plaintext
access-class access-list-name
```

To delete a setting, use the `no access-class` command.

**Parameters**

- `access-list-name` Enter the name of an established IP Standard ACL.

**Defaults**

Not configured.

**Command Modes**

LINE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `line` — applies an authentication method list to the designated terminal lines.
- `ip access-list standard` — names (or selects) a standard access list to filter based on the IP address.
- `ip access-list extended` — names (or selects) an extended access list based on the IP addresses or protocols.
enable password

Change the password for the enable command.

Syntax

enable password [level level] [encryption-type] password

To delete a password, use the no enable password [encryption-type] password [level level] command.

Parameters

- **level level** (OPTIONAL) Enter the keyword level then a number as the level of access. The range is from 1 to 15.
- **encryption-type** (OPTIONAL) Enter the number 7 or 0 as the encryption type.

- Enter a 7 then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.
- Use this parameter only with a password that you copied from the show running-config file of another Dell Networking router.

- **password** Enter a text string, up to 32 characters long, as the clear text password.

Defaults

No password is configured. level = 15.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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:

- A minimum of 8 characters for strong passwords.
- A maximum of 32 characters for default passwords.
- At least one upper case letter (A through Z)
- At least one lower case letter (a through z)
- At least one digit (0 through 9)
- At least one special character from: !@#$%^&*()_=-+|{}:';",.<>/?
- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password "abcd]e", you type "abcd CNTL v ]e". When the password is created, you do not use the CNTL + v key combination and enter "abcd]e".

**NOTE:** The question mark (?) and the tilde (~) are not supported characters.

**Related Commands**
- `show running-config` — views the current configuration.
- `privilege level (CONFIGURATION mode)` — controls access to the command modes within the switch.

### enable sha256-password

Configure SHA-256 based password for the `enable` command.

**Syntax**
```
enable sha256-password [level level] [encryption-type] password
```

To delete a password, use the `no enable sha256-password [encryption-type] password [level level]` command.

**Parameters**
- `sha256-password` Enter the keyword `sha256-password` then the `encryption-type` or the password.
- `level level` (OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
- `encryption-type` (OPTIONAL) Enter the number 8 or 0 as the encryption type.
  - Enter 8 to enter the sha256–based hashed password.
- `password` Enter a text string, up to 32 characters long, as the clear text password.

**Defaults**
No password is configured. `level = 15`.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON, S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, MXL, FN IOM, C9010, S3100, and Z9100–ON.</td>
</tr>
</tbody>
</table>

**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
```

Security | 1305
To disallow access to restricted commands, use the no enable restricted command.

Parameters

**encryption-type**

(Optional) Enter the number 7 as the encryption type.

Enter 7 followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.

Use this parameter only with a password that you copied from the show running-config file of another Dell Networking router.

**password**

Enter a text string, up to 32 characters long, as the clear text password.

Defaults

Not configured.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Only Dell Networking Technical Support staff use this command.

**enable secret**

Change the password for the enable command.

**Syntax**

```
enable secret [level level] [encryption-type] password
```

To delete a password, use the no enable secret [encryption-type] password [level level] command.

**Parameters**

**level level**

(Optional) Enter the keyword level then a number as the level of access. The range is from 1 to 15.

**encryption-type**

(Optional) Enter the number 5 or 0 as the encryption type.
Enter a 5 then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router.

Use this parameter only with a password that you copied from the show running-config file of another Dell Networking router.

```
password
```

Enter a text string, up to 32 characters long, as the clear text password.

**Defaults**

No password is configured. level = 15.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd\]e`, you type `"abcd CNTL v ]e"`. When the password is created, you do not use the CNTL + v key combination and enter `"abcd\]e"`.

**NOTE:** The question mark (?) and the tilde (~) are not supported characters.

**Related Commands**

- `show running-config` — views the current configuration.
- `privilege level (CONFIGURATION mode)` — controls access to the command modes within the switch.
login authentication

To configure authentication for console or remote access, apply an authentication method list.

Syntax

login authentication {method-list-name | default}

To use the local user/password database for login authentication, use the no login authentication command.

Parameters

- **method-list-name**: Enter the keywords method-list-name to specify that method list, created in the aaa authentication login command, to be applied to the designated terminal line.
- **default**: Enter the keyword default to specify that the default method list, created in the aaa authentication login command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines. Local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6.0.0</td>
<td>Revised introductory and usage guidelines description.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If you configure the aaa authentication login default command, the login authentication default command automatically is applied to all terminal lines.

When configuring authentication, consider the following:

- If you configure the default authentication list using the default keyword, the list applies it to all the local and remote connections globally, unless you have specified some another authentication list for a specific connection.
• If you configure an authentication lists other than default, you must apply those authentication lists to each connection.

• If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.

**Related Commands**

- `aaa authentication login` — selects the login authentication methods.

---

### `password`

Specify a password for users on terminal lines.

**Syntax**

```
password [encryption-type] password
```

To delete a password, use the `no password password` command.

**Parameters**

- `encryption-type` (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the password entered. The options are:
  - 0 is the default and means the password is not encrypted and stored as clear text.
  - 7 means that the password is encrypted and hidden.

- `password` Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

**Defaults**

No password is configured.

**Command Modes**

LINE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Networking OS prompts users for these passwords when the method for authentication or authorization used is "line".
Related Commands

- `enable password` — sets the password for the `enable` command.
- `login authentication` — configures an authentication method to log in to the switch.
- `service password-encryption` — encrypts all passwords configured in Dell Networking OS.
- `radius-server key` — configures a key for all RADIUS communications between the switch and the RADIUS host server.
- `tacacs-server key` — configures a key for communication between a TACACS+ server and client.
- `username` — establishes an authentication system based on user names.

**password-attributes**

Configure the password attributes (strong password).

**Syntax**

```
password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]
```

To return to the default, use the `no password-attributes [min-length number] [max-retry number] [lockout-period minutes] [character-restriction [upper number] [lower number] [numeric number] [special-char number]]` command.

**Parameters**

- `min-length 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
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced lockout-period option on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced lockout-period option on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.3.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Example

In the following example, after 5 un-successful login attempts, the session (SSH/TELNET) goes into a locked state for 5 minutes. If all the 10 sessions are locked out with 5 un-successful attempts in each session, no users can login during the lockout-period.

Dell(conf)# password-attributes max-retry 5 lockout-period 5

### Related Commands

- `password` — specifies a password for users on terminal lines.

### service password-encryption

Encrypt all passwords configured in Dell Networking OS.

**Syntax**

```
service password-encryption
```

To store new passwords as clear text, use the `no service password-encryption` command.

**Defaults**

Enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
show privilege

View your access level.

Syntax

show privilege

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

Usage Information

⚠️ 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

Introduction Privilege Level

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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) — assign access control to different command modes.

show users

Allows you to view information on all users logged in to the switch.

Syntax

```
show users [all]
```

Parameters

all (OPTIONAL) Enter the keyword all to view all terminal lines in the switch.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Added support for roles on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Usage Information

The following describes the `show user` command shown in the following example.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(untitled)</td>
<td>Indicates with an asterisk (*) which terminal line you are using.</td>
</tr>
<tr>
<td>Line</td>
<td>Displays the terminal lines currently in use.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the user name of all users logged in.</td>
</tr>
<tr>
<td>Host(s)</td>
<td>Displays the terminal line status.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the IP address of the user.</td>
</tr>
</tbody>
</table>

Example

```
Dell# show users
Authorization Mode: role or privilege

Line             User                      Role             Priv
Host(s) Location
* 0  console 0   admin                     unassigned         1 idle
  2 vty 0         unassigned                1
  3 vty 1         ad                         unassigned        15 idle
  4 vty 2         ad1                        sysadmin           1 idle
  5 vty 3         ad1                        sysadmin           1
  6 vty 4         ad                         unassigned        1 idle
  7 vty 5         ad1                        sysadmin           1
  8 vty 6         adilateral                unassigned        15 idle

Dell#
```

Related Commands

- `username` — enables a user.

### timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

**Syntax**

```
timeout login response seconds
```

To return to the default values, use the `no timeout login response` command.

**Parameters**

- `seconds`
  
  Enter a number of seconds the software waits before logging you out. The range is:
  
  - VTY — range is from 1 to 30 seconds, the default is **30 seconds**.
  - Console — range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).
  - AUX — range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).

**Defaults**

See Parameters.

**Command Modes**

LINE
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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**

- **name**: Enter a text string for the name of the user up to 63 characters.

- **access-class access-list-name**: Enter the keywords `access-class` then the name of a configured access control list (either an IP access control list or MAC access control list).

- **nopassword**: Enter the keyword `nopassword` to specify that the user should not enter a password.

- **password**: Enter the keyword `password` then the encryption-type or the password.

- **encryption-type**: Enter an encryption type for the password that you enter.

  - 0 directs the system to store the password as clear text. It is the default encryption type when using the `password` option.
  - 8 to indicate that a password encrypted using a sha256 hashing algorithm follows. This encryption type is available with the `sha256-password` option only, and is the default encryption type for this option.
• 7 to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the password option only.
• 5 to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is available with the secret option only, and is the default encryption type for this option.

password
Enter a string up to 32 characters long.

privilege level
Enter the keyword privilege then a number from zero (0) to 15.

role role-name
Enter the keyword role followed by the role name to associate with that user ID.

secret
Enter the keyword secret then the encryption type.

sha256-password
Enter the keyword sha256-password then the encryption-type or the password.

Defaults
The default encryption type for password option is 0. The default encryption type for secret option is 5. The default encryption type for sha256-password option is 8. The default value of privilege level is 1.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Added support for the sha256-password option for S3100, S3048-ON, S4048-ON, S4810, S4820T, S5000, S6000, S6000-ON, Z9100-ON, MXL, and Z9500.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.0) Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.7.1.0 Added support for the secret option and the MD5 password encryption. Extended the name from 25 to 63 characters.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

Usage Information
To view the defined user names, use the show running-config user command.

Related Commands
• password — specifies a password for users on terminal lines.
• enable sha256-password — configures SHA-256 based password.
• show running-config — views the current configuration.
### RADIUS Commands

The following RADIUS commands are supported by Dell Networking OS.

#### debug radius

View RADIUS transactions to assist with troubleshooting.

**Syntax**
```
debug radius
```

To disable debugging of RADIUS, use the `no debug radius` command.

**Defaults**
Disabled.

**Command Modes**
EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

#### ip radius source-interface

Specify an interface’s IP address as the source IP address for RADIUS connections.

**Syntax**
```
ip radius source-interface interface
```

To delete a source interface, use the `no ip radius source-interface` command.

**Parameters**

- `interface` Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.

For a port channel interface, enter the keywords port-channel then a number.

For a Null interface, enter the keyword null then the Null interface number.

For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
radius-server group

Creates or deletes a group of radius servers.

Syntax

radius-server group group-name

Parameters

group-name

Enter the group name that denotes the group of RADIUS servers.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
prefix-6.1.1.0 Introduced on the E-Series.

Example

Dell(conf)# radius-server group group1
Dell(conf-radius-group)# radius-server host 1.1.1.1 key secret
Dell(conf-radius-group)# radius-server host 2.2.2.2 key secret
Dell(conf-radius-group)# radius-server vrf vrf1 source-interface gigabitethernet 1/36
Dell(conf-radius-group)# show config
!
radius-server group group1
radius-server vrf vrf1 source-interface gigabitEthernet 1/36
radius-server host 1.1.1.1 key 7 9a2f3ec0c65c6f41
radius-server host 2.2.2.2 key 7 9a2f3ec0c65c6f41
Dell(conf-radius-group)#

Related Commands
- login authentication — sets the database to be checked when a user logs in.
- radius-server key — sets an authentication key for RADIUS communications.
- radius-server retransmit — sets the number of times the RADIUS server attempts to send information.
- radius-server timeout — sets the time interval before the RADIUS server times out.

radius-server host
Configure a RADIUS server host.

Syntax
radius-server host {hostname | ipv4-address | ipv6-address} [auth-port port-number] [retransmit retries] [timeout seconds] [key [encryption-type] key]

Parameters
- hostname Enter the name of the RADIUS server host.
- ipv4-address | ipv6-address Enter the IPv4 address (A.B.C.D) or IPv6 address (X::X::X::X) of the RADIUS server host.
- auth-port port-number (OPTIONAL) Enter the keywords auth-port then a number as the port number. The range is from zero (0) to 65535. The default port-number is 1812.
- retransmit retries (OPTIONAL) Enter the keyword retransmit then a number as the number of attempts. This parameter overwrites the radius-server retransmit command. The range is from zero (0) to 100. The default is 3 attempts.
- timeout seconds (OPTIONAL) Enter the keyword timeout then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the radius-server timeout command. The range is from 0 to 1000. The default is 5 seconds.
- key [encryption-type] key (OPTIONAL) Enter the keyword key then an optional encryption-type and a string up to 42 characters long as the authentication key. The RADIUS host server uses this authentication key and the RADIUS daemon operating on this switch. For the encryption-type, enter either zero (0) or 7 as the encryption type for the key entered. The options are:
  - 0 is the default and means the password is not encrypted and stored as clear text.
  - 7 means that the password is encrypted and hidden.
Configure this parameter last because leading spaces are ignored.

Defaults
Not configured.

Command Modes
- RADIUS SERVER GROUP
- 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
---|---
9.8(1.0) | Introduced on the Z9100-ON.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Authentication key length increased to 42 characters.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

To configure any number of RADIUS server hosts for each server host that is configured, use this command. Dell Networking OS searches for the RADIUS hosts in the order they are configured in the software.

The global default values for the `timeout`, `retransmit`, and `key` optional parameters are applied, unless those values are specified in the `radius-server host` or other commands. To return to the global default values, if you configure the `timeout`, `retransmit`, or `key` values, include those keywords when using the `no radius-server host` command syntax.

You can use duplicate host names or IP addresses among RADIUS groups. However, you cannot use duplicate host names or IP addresses within the same RADIUS group. If a VRF is not configured on the RADIUS group, then servers configured in the group are considered to be on the default VRF. RADIUS servers that are configured in the CONFIGURATION mode are also considered to be on the default VRF.

You must configure the RADIUS group explicitly with the `aaa radius group` command in order for the AAA servers to use the group of RADIUS servers. The 802.1x servers use the group of RADIUS servers based on the VRF where the 802.1x request is received. As a result, it is possible that both globally configured RADIUS servers as well as the group-configured RADIUS servers (without VRF or default VRF) are used for processing the 802.1x requests that are received at the default VRF. The order in which the RADIUS servers are tried depends on the order in which the RADIUS servers are configured.

**Example**

```
Dell(conf)# radius-server group group1
Dell(conf-radius-group)# radius-server host 1.1.1.1 key secret
Dell(conf-radius-group)# no radius-server host 1.1.1.1
Dell(conf-radius-group)#
```

**Related Commands**

- `login authentication` — sets the database to be checked when a user logs in.
- `radius-server key` — sets an authentication key for RADIUS communications.
- `radius-server retransmit` — sets the number of times the RADIUS server attempts to send information.
- `radius-server timeout` — sets the time interval before the RADIUS server times out.
radius-server vrf

Create an association between a RADIUS server group and a VRF and source interface.

Syntax

radius-server vrf vrf-name [source-interface interface]

To delete the association between a RADIUS server group and a VRF and source interface, use the no radius-server vrf vrf-name [source-interface interface] command.

Parameters

vrf vrf-name
Enter the keyword vrf and then the name of the VRF to associate a RADIUS server group with that VRF.

interface
Enter the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

RADIUS SERVER GROUP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.2(1.0) Introduced on the Z9500.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.0) Introduced on the Z9500.
9.4(0.0) Introduced on the S-Series and Z9000.

Usage Information

You can use this command to associate a group of RADIUS servers with a VRF and source interface. You can configure the source interface only with the VRF attribute and source interface is optional with the VRF attributes.

If VRF is not configured on the RADIUS group, then the group is considered to be on the default VRF. It is possible to use the default VRF name; however, you cannot configure the source interface with the default VRF as such a configuration results in conflicts between the source interfaces corresponding to the 802.1x supplicants on that default VRF.
RADIUS groups and VRFs have one-to-one mapping. If a VRF is configured with one RADIUS group, then you cannot use the same VRF with another RADIUS group. When the VRF is removed, then the corresponding RADIUS group is also removed automatically.

Example

Dell(conf)#radius-server group group1
Dell(conf-radius-group)#radius-server vrf vrf1 source-interface gigabitethernet 1/42
Dell(conf)#radius-server group group2
Dell(conf-radius-group)#radius-server vrf default

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

Syntax

radius-server key [encryption-type] key

To delete a password, use the no radius-server key command.

Parameters

encryption-type  (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered. The options are:

- 0 is the default and means the key is not encrypted and stored as clear text.
- 7 means that the key is encrypted and hidden.

key  Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults  Not configured.

Command Modes  CONFIGURATION

Command History  This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Authentication key length increased to 42 characters.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
pre-6.2.1.0 | Introduced on the E-Series.

**Usage Information**
The key configured on the switch must match the key configured on the RADIUS server daemon.

If you configure the key parameter in the radius-server host command, the key configured with the radius-server key command is the default key for all RADIUS communications.

**Related Commands**
- radius-server host — configures a RADIUS host.

### radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

**Syntax**
radius-server retransmit retries

To configure zero retransmit attempts, use the no radius-server retransmit command.

To return to the default setting, use the radius-server retransmit 3 command.

**Parameters**

- **retries**
  
Enter a number of attempts that the Dell OS tries to locate a RADIUS server. The range is from zero (0) to 100. The default is 3 retries.

**Defaults**

3 retries

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
radius-server timeout

To reply to a request, configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server.

Syntax

radius-server timeout seconds

To return to the default value, use the no radius-server timeout command.

Parameters

- **seconds**
  Enter the number of seconds between an unsuccessful attempt and the Dell Networking OS times out. The range is from zero (0) to 1000 seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- **radius-server host** — configure a RADIUS host.
TACACS+ Commands

Dell Networking OS supports TACACS+ as an alternate method for login authentication.

tacacs-server group

Creates a group of TACACS servers to be used for Authentication, Authorization, and Accounting.

Syntax

```
aaa tacacsgroup group-name
```

To delete a group of TACACS servers, use the `no tacacs-server group group-name` command.

Parameters

- **group-name**
  
Enter the name of the TACACS server group.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If the TACACS group is not configured for Authentication, Authorization, and Accounting, then globally configured TACACS servers are used for the purposes. When the TACACS group is removed, the AAA configuration is also removed.

Example

```
Dell(conf)# tacacs-server group group1
Dell(conf-tacacs-group)# tacacs-server host 1.1.1.1 key secret
Dell(conf-tacacs-group)# tacacs-server host 2.2.2.2 key secret
Dell(conf-tacacs-group)# tacacs-server vrf vrf1 source-interface gigabitethernet 1/40
Dell(conf)# exit
Dell(conf)# aaa tacacsgroup group1
```

Related Commands

- `aaa authentication login` — specifies the login authentication method.
- `tacacs-server key` — configures a TACACS+ key for the TACACS server.
**debug tacacs+**

To assist with troubleshooting, view TACACS+ transactions.

**Syntax**

```
debug tacacs+
```

To disable debugging of TACACS+, use the `no debug tacacs+` command.

**Defaults**

Disabled.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**ip tacacs source-interface**

Specify an interface’s IP address as the source IP address for TACACS+ connections.

**Syntax**

```
ip tacacs source-interface interface
```

To delete a source interface, use the `no ip tacacs source-interface` command.

**Parameters**

`interface`  
Enter the following keywords and the interface information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**tacacs-server group**

Creates a group of TACACS servers.

**Syntax**

```
tacacs-server group group-name
```

To delete a group of TACACS servers, use the `no tacacs-server group group-name` command.

**Parameters**

- `group-name` Enter the name of the TACACS server group.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
</tbody>
</table>
tacacs-server host

Specify a TACACS+ host.

Syntax

```
tacacs-server host {hostname | ipv4-address | ipv6-address} [port number] [timeout seconds] [key key]
```

Parameters

- **hostname**
  - Enter the name of the TACACS+ server host.

- **ipv4-address | ipv6-address**
  - Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the TACACS+ server host.

- **port number**
  - (OPTIONAL) Enter the keyword port then a number as the port to be used by the TACACS+ server. The range is from zero (0) to 65535. The default is 49.

- **timeout seconds**
  - (OPTIONAL) Enter the keyword timeout then the number of seconds the switch waits for a reply from the TACACS+ server. The range is from 0 to 1000. The default is 10 seconds.

- **key key**
  - (OPTIONAL) Enter the keyword key then a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the `tacacs-server key` for the TACACS+ daemon.

Defaults

Not configured.

Command Modes

**CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(10)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Authentication key length increased to 42 characters.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Added support for IPv6.</td>
</tr>
</tbody>
</table>

**Usage Information**

To list multiple TACACS+ servers to be used by the `aaa authentication login` command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the `port`, `timeout`, and `key` optional parameters. If you do not configure a key, the key assigned in the `tacacs-server key` command is used.

You can use duplicate host names or IP addresses among TACACS groups. However, you cannot use duplicate host names or IP addresses within the same TACACS group.

If a VRF is not configured on the TACACS group, then servers configured in the group are considered to be on the default VRF. TACACS servers that are configured in the CONFIGURATION mode are also considered to be on the default VRF.

For AAA servers to use a group of TACACS servers, you must explicitly configure the group using the `aaa tacacs group group-name` command. The order in which the TACACS servers are tried depends on the order in which they are configured.

**Example**

```bash
Dell(conf)# tacacs-server group group1
Dell(conf-tacacs-group)# tacacs-server host 1.1.1.1 key secret
Dell(conf-tacacs-group)# no tacacs-server host 1.1.1.1
Dell(conf-tacacs-group)#
```

**Related Commands**

- `aaa authentication login` — specifies the login authentication method.
- `tacacs-server key` — configures a TACACS+ key for the TACACS server.

---

**tacacs-server key**

Configure a key for communication between a TACACS+ server and a client.

**Syntax**

```
tacacs-server key [encryption-type] key
```
To delete a key, use the `no tacacs-server key key` command.

**Parameters**

- `encryption-type` (OPTIONAL) Enter either zero (0) or 7 as the encryption type for the key entered. The options are:
  - 0 is the default and means the key is not encrypted and stored as clear text.
  - 7 means that the key is encrypted and hidden.

- `key` Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000--ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Authentication key length increased to 42 characters.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The key configured with this command must match the key configured on the TACACS+ daemon.

### tacacs-server vrf

Create an association between a TACACS server group and a VRF and source interface.

**Syntax**

```
tacacs-server vrf vrf-name [source-interface interface]
```

To delete the association between a TACACS server group and a VRF and source interface, use the `no tacacs-server vrf vrf-name [source-interface interface]` command.

**Parameters**

- `vrf vrf-name` Enter the keyword `vrf` and then the name of the VRF to associate a TACACS server group with that VRF.

- `interface` Enter the following keywords and slot/port or number information:
• For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
• For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
• For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
• For a port channel interface, enter the keywords port-channel then a number.
• For a Null interface, enter the keyword null then the Null interface number.
• For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
TACACS SERVER GROUP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Introduced on the S-Series and Z-Series.</td>
</tr>
</tbody>
</table>

Usage Information
You can use this command to associate a group of TACACS servers with a VRF and source interface. You can
configure the source interface only with the VRF attribute and source interface is optional with the VRF attributes.

If VRF is not configured on the TACACS group, then the group is considered to be on the default VRF.

RADIUS groups and VRFs have one-to-one mapping. If a VRF is configured with one RADIUS group, then you
cannot use the same VRF with another RADIUS group. When the VRF is removed, then the corresponding
RADIUS group is also removed automatically.

Example
Dell(conf)# tacacs-server group group1
Dell(conf-tacacs-group)# tacacs-server vrf vrf1 source-interface gigabitethernet 1/36
Dell(conf)# tacacs-server group group2
Dell(conf-tacacs-group)# tacacs-server vrf default

Port Authentication (802.1X) Commands

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only Extensible
Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is
successful, normal traffic passes through the port.

Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.
Important Points to Remember

Dell Networking OS limits network access for certain users by using VLAN assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is supported on Dell Networking OS.
- 802.1X is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

dot1x authentication (Configuration)

Enable dot1x globally; dot1x must be enabled both globally and at the interface level.

Syntax

dot1x authentication

To disable dot1x on globally, use the no dot1x authentication command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
(Configuration) — enable dot1x globally.

Related Commands

- **dot1x auth-fail-vlan**

Configures an authentication failure VLAN for users and devices that fail 802.1X authentication.

**Syntax**

```
dot1x auth-fail-vlan vlan-id [max-attempts number]
```

**Parameters**

- `vlan-id` Enter the VLAN Identifier. The range is from 1 to 4094.
- `max-attempts number` (Optional) Enter the keywords `max-attempts` then number of attempts desired before authentication fails. The range is from 1 to 5. The default is 3.
Defaults
3 attempts

Command Modes
CONFIGURATION (conf-if-interface-slot/port)

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series, S-Series, and E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface is moved to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next re-authentication interval (dot1x reauthentication).

Related Commands
- `dot1x port-control` — enables port-control on an interface.
- `dot1x guest-vlan` — configures a guest VLAN for non-dot1x devices.
- `show dot1x interface` — displays the 802.1X information on an interface.

**dot1x auth-server**

Configure the authentication server to RADIUS.

**Syntax**

```
dot1x auth-server radius
```

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

Syntax

```
dot1x guest-vlan vlan-id
```

To disable the guest VLAN, use the no dot1x guest-vlan vlan-id command.

Parameters

- **vlan-id**: Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults

Not configured.

Command Modes

- CONFIGURATION (conf-if-interface-slot/port)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication for the device occurs at the next re-authentication interval (dot1x reauthentication).
If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (dot1x auth-fail-vlan).

**NOTE:** The layer 3 portion of guest VLAN and authentication fail VLANs can be created regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands
- `dot1x auth-fail-vlan` — configures a VLAN for authentication failures.
- `dot1x reauthentication` — enables periodic re-authentication.
- `show dot1x interface` — displays the 802.1X information on an interface.

## dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, Dell Networking OS attempts to authenticate the host based on its MAC address.

**Syntax**
```
[no] dot1x mac-auth-bypass
```

**Defaults**
Disabled

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.4</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
To disable MAC authentication bypass on a port, enter the `no dot1x mac-auth-bypass` command.

## dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

**Syntax**
```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.
Parameters  
**number**  Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is 2.

Defaults  
2

Command Modes  
INTERFACE

Command History  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Related Commands  
- interface range — configure a range of interfaces.

**dot1x port-control**

Enable port control on an interface.

**Syntax**  
dot1x port-control {force-authorized | auto | force-unauthorized}

**Parameters**  
- **force-authorized**  Enter the keywords force-authorized to forcibly authorize a port.
- **auto**  Enter the keyword auto to authorize a port based on the 802.1X operation result.
- **force-unauthorized**  Enter the keywords force-unauthorized to forcibly de-authorize a port.

**Defaults**  
none

**Command Modes**  
INTERFACE

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
**dot1x quiet-period**

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

**Syntax**
```
dot1x quiet-period seconds
```

To disable quiet time, use the `no dot1x quiet-time` command.

**Parameters**
- **seconds**
  Enter the number of seconds. The range is from 1 to 65535. The default is **30**.

**Defaults**
**30 seconds**

**Command Modes**
**INTERFACE**

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

**Version** | **Description**
---|---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the C-Series and S-Series.
7.4.1.0 | Introduced on the E-Series.

**Usage Information**
The authenticator performs authentication only when `port-control` is set to `auto`.

---

**Version** | **Description**
---|---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the C-Series and S-Series.
7.4.1.0 | Introduced on the E-Series.
**dot1x reauthentication**

Enable periodic re-authentication of the client.

**Syntax**

```
dot1x reauthentication [interval seconds]
```

To disable periodic re-authentication, use the `no dot1x reauthentication` command.

**Parameters**

- `interval seconds` (Optional) Enter the keyword `interval` then the interval time, in seconds, after which re-authentication is initiated. The range is from 1 to 31536000 (1 year). The default is 3600 (1 hour).

**Defaults**

3600 seconds (1 hour)

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `interface range` — configures a range of interfaces.

**dot1x reauth-max**

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

**Syntax**

```
dot1x reauth-max number
```

To return to the default, use the `no dot1x reauth-max` command.

**Parameters**

- `number` Enter the permitted number of re-authentications. The range is from 1 to 10. The default is 2.
dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

Syntax

 dot1x server-timeout seconds

To return to the default, use the no dot1x server-timeout command.

Parameters

seconds Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30.

Defaults 30 seconds

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

Syntax

```
dot1x supplicant-timeout seconds
```

To return to the default, use the `no dot1x supplicant-timeout` command.

Parameters

- `seconds` Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is 30.

Defaults

- **30 seconds**

Command Modes

- INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

dot1x tx-period

Configure the intervals at which EAPOL PDUs are transmitted by the Authenticator PAE.

Syntax

```
dot1x tx-period seconds
```

To return to the default, use the `no dot1x tx-period` command.
**Parameters**

**seconds**  
Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535 (1 year). The default is **30**.

**Defaults**  
**30 seconds**

**Command Modes**  
**INTERFACE**

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**show dot1x interface**

Display the 802.1X information on an interface.

**Syntax**

```
show dot1x interface interface
```

**Parameters**

**interface**  
Enter one of the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword **GigabitEthernet** then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** then the slot/port information.
- For a Loopback interface, enter the keyword **loopback** then a number from 0 to 16383.

**Defaults**  
none

**Command Modes**

- EXEC
- EXEC privilege

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*. 
**Example**

```
Dell# show dot1x interface tengigabitethernet 1/49

802.1x information on Te 1/49:
-----------------------------
Dot1x Status:             Enable
Port Control:             AUTO
Port Auth Status:         UNAUTHORIZED
Re-Authentication:       Disable
Untagged VLAN id:          None
Guest VLAN:               Disable
Guest VLAN id:             NONE
Auth-Fail VLAN:           Disable
Auth-Fail VLAN id:        NONE
Auth-Fail Max-Attempts:   NONE
Mac-Auth-Bypass:          Disable
Mac-Auth-Bypass Only:     Disable
Tx Period:                30 seconds
Quiet Period:             60 seconds
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth interval:         3600 seconds
Max-EAP-Req:              2
Host Mode:                SINGLE_HOST
Auth PAE State:           Initialize
Backend State:            Initialize
Dell#
```

```
Dell# show dot1x interface tengigabitethernet 1/49

802.1x information on Te 1/49:
-----------------------------
Dot1x Status:             Enable
Port Control:             FORCE_AUTHORIZED
Port Auth Status:         UNAUTHORIZED
Re-Authentication:       Disable
Untagged VLAN id:          None
Guest VLAN:               Disable
Guest VLAN id:             NONE
Auth-Fail VLAN:           Disable
Auth-Fail VLAN id:        NONE
Auth-Fail Max-Attempts:   NONE
Mac-Auth-Bypass:          Disable
Mac-Auth-Bypass Only:     Disable
Tx Period:                30 seconds
Quiet Period:             60 seconds
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth interval:         3600 seconds
Max-EAP-Req:              2
Host Mode:                SINGLE_HOST
Auth PAE State:           Initialize
Backend State:            Initialize
Dell#
```
**SSH and SCP Commands**

Dell Networking OS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

### crypto key generate

Generate keys for the SSH server.

**Syntax**

```
crypto key generate {rsa | rsa1}
```

**Parameters**

- `rsa`  
  Enter the keyword `rsa` then the key size to generate a SSHv2 RSA host keys. The range is from 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is 1024.

  - **NOTE:** You must have a license to access the FIPS mode. For more information, contact your Dell Networking representative.

- `rsa1`  
  Enter the keyword `rsa` then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048. The default is 1024.

  - **NOTE:** This option is not available in FIPS mode.

**Defaults**

Key size 1024: If you enable FIPS mode, the key size is 2048.

**Command Modes**

- **CONFIGURATION**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
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.

```
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)#
```

Example

```
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.

### crypto key zeroize rsa

Removes the generated RSA host keys and zeroize the key storage location.

**Syntax**

```
crypto key zeroize rsa
```

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9000, S6000, S4820T, S4810, MXL</td>
</tr>
</tbody>
</table>
**debug ip ssh**

Enables collecting SSH debug information.

Syntax

```
debug ip ssh {client | server}
```

To disable debugging, use the `no debug ip ssh {client | server}` command.

Parameters

- **client**: Enter the keyword `client` to enable collecting debug information on the client.
- **server**: Enter the keyword `server` to enable collecting debug information on the server.

Defaults

Disabled on both client and server.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Debug information includes details for key-exchange, authentication, and established session for each connection.

**ip scp topdir**

Identify a location for files used in secure copy transfer.

Syntax

```
ip scp topdir directory
```

To return to the default setting, use the `no ip scp topdir` command.

Parameters

- **directory**: Enter a directory name.

Defaults

The internal flash (`flash:`) is the default directory.
Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
To configure the switch as an SCP server, use the ip ssh server command.

Related Commands
- `ip ssh server` — enables the SSH and SCP server on the switch.

**ip ssh authentication-retries**

Configure the maximum number of attempts that should be used to authenticate a user.

**Syntax**

```
ip ssh authentication-retries 1-10
```

**Parameters**

- `1-10` 
Enter the number of maximum retries to authenticate a user. The range is from 1 to 10. The default is 3.

**Defaults**

3

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

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.
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**

```plaintext
ip ssh connection-rate-limit 1-10
```

**Parameters**

- `1-10`  
  Enter the number of maximum numbers of incoming SSH connections allowed per minute. The range is from 1 to 10 per minute. The default is **10 per minute**.

**Defaults**

**10 per minute**

**Command Modes**

**CONFIGURATION**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
pre-6.11.0 | Introduced on the E-Series.
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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000--ON.

9.2(1.0) Introduced on the Z9500.

9.0.2.0 Introduced on the S6000.

8.3.19.0 Introduced on the S4820T.

8.3.11.1 Introduced on the Z9000.

8.3.7.0 Introduced on the S4810.

7.6.1.0 Introduced on the S-Series.

7.5.1.0 Introduced on the C-Series.

pre-6.1.1.0 Introduced on the E-Series.

Usage Information

If you enable this command, clients can log in without a password prompt. This command provides two levels of authentication:

- rhost-authentication is done with the file specified in the ip ssh rhostfile command.
- checking client host-keys is done with the file specified in the ip ssh pub-key-file command.

NOTE: Administrators must specify the two files (rhosts and pub-key-file) to configure host-based authentication.

Related Commands

- ip ssh pub-key-file — public keys of trusted hosts from a file.
- ip ssh rhostsfile — trusted hosts and users for rhost authentication.
ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

Syntax

ip ssh key-size 512-869

Parameters

512-869 Enter the key-size number for the server-generated RSA SSHv1 key. The range is from 512 to 869. The default is 768.

Defaults
Key size 768

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

Usage Information
The server-generated key is used for SSHv1 key-exchange.

ip ssh 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-shal

Security

1352
• hmac-sha1-96

When FIPS mode is disabled:
• hmac-sha2-256
• hmac-sha1
• hmac-sha1-96
• hmac-md5
• hmac-md5-96

When FIPS mode is enabled:
• hmac-sha2-256
• hmac-sha1
• hmac-sha1-96

The default list of MAC algorithm is in the order as shown below:

The default list of MAC algorithm is in the order as shown below:

When FIPS mode is disabled:
• hmac-sha2-256
• hmac-sha1
• hmac-sha1-96
• hmac-md5
• hmac-md5-96

When FIPS mode is enabled:
• hmac-sha2-256
• hmac-sha1
• hmac-sha1-96

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.

Syntax
ip ssh password-authentication enable

To disable password-authentication, use the no ip ssh password-authentication enable command.

Parameters
enable Enter the keyword enable to enable password-authentication for the SSH server.
Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.

**ip ssh pub-key-file**

Specify the file used for host-based authentication.

**Syntax**

ip ssh pub-key-file \{WORD\}

**Parameters**

WORD Enter the file name for the host-based authentication.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
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 AAAAB3NzaC1yc2EAAAABBIwAAAIEAox/QQP8xYhz0xN07yh4VGPu6UfkgKoieTH9G4sNV+ui+DFEc3cgyAc5LaU1MU2ODrzhCwyDNp05tKBU3tReGl08xLil6+54hyEMgHxkzBFNvqHzpQC
+RsD42urzV0FpBrKnaXk3Lk4640H2ZhVrXqenNDpEn WIMPJi0ds= ashwani@poclab4
```

**NOTE:** For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the chassis.

Example

```
Dell# conf
Dell(conf)# ip ssh pub-key-file flash://knownhosts
Dell(conf)#
```

Related Commands

- `show ip ssh client-pub-keys` — displays the client-public keys used for the host-based authentication.

**ip ssh rekey**

Configures the time rekey-interval or volume rekey-limit threshold at which to re-generate the SSH key during an SSH session.

**Syntax**

```
ip ssh rekey [time rekey-interval] [volume rekey-limit]
```

To reset to the default, use no `ip ssh rekey [time rekey-interval] [volume rekey-limit]` command.

**Parameters**

- `time rekey-interval`
  - Enter the keywords `time` then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is 60 minutes
  - `volume rekey-limit`
  - Enter the keywords `volume` then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is 1024 megabytes

**Defaults**

- The default time is 60 minutes. The default volume is 1024 megabytes.

**Command Modes**

- CONFIGURATION mode
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9000, S6000, S4820T, S4810, MXL</td>
</tr>
</tbody>
</table>

**ip ssh rhostsfile**

Specify the rhost file used for host-based authorization.

**Syntax**

```
ip ssh rhostsfile {WORD}
```

**Parameters**

<table>
<thead>
<tr>
<th>WORD</th>
<th>Enter the rhost file name for the host-based authentication.</th>
</tr>
</thead>
</table>

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell#conf
Dell(conf)# ip ssh rhostsfile flash://shosts
Dell(conf)#
```
This command specifies the rhost file used for host-based authentication. This command creates/overwrites the flash:/ADMIN_DIR/ssh/shosts file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.

**NOTE:** For rhostfile and pub-key-file, the administrator must FTP the file to the switch.

### ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

**Syntax**

```plaintext
ip ssh rsa-authentication enable
```

To disable RSA authentication, use the no ip ssh rsa-authentication enable command.

**Parameters**

- `enable` Enter the keyword `enable` to enable RSA authentication for the SSHv2 server.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Enabling RSA authentication allows the user to log in without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (ip ssh rsa-authentication my-authorized-keys device://filename command).
**ip ssh server**

Configure an SSH server. SSH server is enabled by default.

**Syntax**

```bash
ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]
```

To disable SSH server functions, use the `no ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]` command.

**Parameters**

- **enable**
  - Enter the key word `enable` to start the SSH server.

- **ciphers cipher-list**
  - Enter the keyword `ciphers` and then a space-delimited list of ciphers that the SSH server supports. The following ciphers are available:
    - 3des-cbc
    - aes128-cbc
    - aes192-cbc
    - aes256-cbc
    - aes128-ctr
    - aes192-ctr
    - aes256-ctr
  - The default cipher list is used.

- **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

**NOTE:** Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.
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-shal
- hmac-shal-96
- hmac-sha2-256

**kex key-exchange-algorithm**

Enter the keyword `kex` and then a space-delimited list of key exchange algorithms supported by the SSH server.

The following key exchange algorithms are available:
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1

When FIPS is enabled, the default key-exchange-algorithm is diffie-hellman-group14-sha1.

When FIPS is not enabled, the default key-exchange-algorithms are the following:
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1

**port port-number**

(Optional) Enter the keyword `port` then the port number of the listening port of the SSH server. The range is from 1 to 65535. The default is 22.

**[version {1 | 2}]**

(Optional) Enter the keyword `version` then the SSH version 1 or 2 to specify only SSHv1 or SSHv2.

**NOTE:** If you enable FIPS mode, you can only select version 2.

**Defaults**
- Default listening port is 22.
- Default cipher list is 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr.
- When FIPS is enabled, the default is hmac-sha1-96.
- When FIPS is not enabled, the default is hmac-md5,hmac-md5-96,hmac-shal,hmac-sha1-96,hmac-sha2-256.
- When FIPS is enabled, the default is diffie-hellman-group14-sha1.
- When FIPS is not enabled, the default is diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1.

**Command Modes**
- CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### Version Description

9.10(0.0) Removed the support for hmac-sha2-256-96 algorithm.
9.8(2.0) Introduced on the S3100 series.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced the cipher, kex and mac options on the Z9500.
9.5(0.0) Introduced the cipher, kex and mac options on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
pre-6.1.1.0 Introduced on the E-Series.

### Usage Information

This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

**NOTE:** Starting with Dell Networking OS Release 9.2(0.0), SSH server is enabled by default.

### Example

```bash
Dell# conf
Dell(conf)# ip ssh server port 45
Dell(conf)# ip ssh server enable
Dell#
```

### Related Commands

- `show ip ssh`

### ip ssh server vrf

Configure an SSH server on either a specific VRF or a management VRF.

#### Syntax

```bash
ip ssh server vrf {management | vrf-name}
```

To disable the SSH server configuration, use the `no ip ssh server vrf {management | vrf-name}` command.

#### Parameters

- `vrf management` Enter the keyword `vrf` followed by the keyword `management` to configure an SSH server on a management VRF.
vrf vrf-name

Enter the keyword vrf followed by the VRF name to configure an SSH server on that VRF.

Defaults
None

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.4(0.0) Introduced on the S-Series and Z9000.

Usage Information
You can enable the SSH server on either a management VRF or a user defined VRF but not both. If no VRF is specified, then the SSH server is enabled on the default VRF.

If the SSH server is enabled on a VRF with name vrf1, then use the following command to restart the SSH server on a VRF with name vrf2: ip ssh server vrf vrf2. If the SSH server is enabled on a VRF with name vrf1, then use the following command to restart the SSH server on the default VRF: ip ssh server vrf.

Example
• Dell(conf)# ip ssh server vrf vrf1
• Dell(conf)# no ip ssh server vrf
• Dell(conf)# ip ssh server vrf management
• Dell(conf)# no ip ssh server vrf

Related Commands
• show ip ssh — displays the ssh information.

ip ssh source-interface

Specifies an interface's IP address as the source IP address for an outgoing SSH connections.

Syntax
ip ssh source-interface interface
To delete a source interface, use the no ip ssh source-interface command.

Parameters
interface

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.
Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information
The source-interface interface attribute is applicable for both the SSH client as well as the COPY (SCP) commands. Using these attributes the client session tags an error to the user during run time, in case there is a mismatch between this command and the ip ssh vrf command.

Example
Dell(conf)#ip ssh source-interface gigabitethernet 1/47
Dell(conf)#do ssh 10.10.10.2 -l admin
Dell(conf)#no ip ssh source-interface

ip ssh vrf

Specify a VRF for an outgoing SSH connections.

Syntax
ip ssh vrf vrf-name

To delete a VRF for an outgoing SSH connection, use the no ip ssh vrf vrf-name command.

Parameters
vrf vrf-name Enter the keyword vrf and then the name of the VRF to configure that VRF for an outgoing SSH session.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
**Usage Information**

If you configure a VRF for an SSH session, then you need not explicitly mention the same VRF for the SSH client sessions intended for that VRF. The vrf attribute in the `ip ssh vrf` command is applicable for both the SSH client as well as the COPY (SCP) commands.

**Example**

```plaintext
Dell(conf)#ip ssh vrf vrf1
Dell(conf)#do ssh 10.10.10.2 -l admin
Dell(conf)#no ip ssh vrf vrf1
```

**show crypto**

Display the public part of the SSH host-keys.

**Syntax**

```plaintext
show crypto key mypubkey {rsa | rsa1}
```

**Parameters**

- **Key**
  - Enter the keyword key to display the host public key.
- **mypubkey**
  - Enter the keyword mypubkey to display the host public key.
- **rsa**
  - Enter the keyword rsa to display the host SSHv2 RSA public key.
- **rsa1**
  - Enter the keyword rsa1 to display the host SSHv1 RSA public key.

**Defaults**

none

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.4(0.0) | Introduced on the S-Series and Z9000.

9.8(1.0) | Introduced on the Z9100-ON.

9.8(0.0P5) | Introduced on the S4048-ON.

9.8(0.0P2) | Introduced on the S3048-ON.

9.7(0.0) | Introduced on the S6000-ON.

9.2(1.0) | Introduced on the Z9500.

9.0.2.0 | Introduced on the S6000.

8.3.11.1 | Introduced on the Z9000.

8.3.7.0 | Introduced on the S4810.

7.6.1.0 | Introduced on the S-Series.

7.5.1.0 | Introduced on the C-Series.
show ip ssh

Display information about established SSH sessions.

Syntax

```
show ip ssh
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Removed the support for hmac-sha2-256-96 algorithm.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

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 15047757832969676203444203678896349387088507047999199481529
20706267059651487389873388513888726045587485998010070732182414929030
69202754303379333684808165031718757388498171624789466770656068362720
77109398066281380715348265219018664332445168871204153163024573977444960433536430225148130737348756957374121

Dell# show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCIYgcUcc8wQm+5KUQgW/zAs8V5STalQg4/+S+6H9axpQnA+A0xweec5iR5hvPF6Vc+HS+uWcQH+/VOJ8H5Jxsm347XnYv/gpSqhjJ2/C5UwFlucVkVfYu8RDCJVIuQhlVvPEebIF5Q+sD8K89MX90MAs/UdoiJZ8O11baCuSTW1Q==

Dell#
```

Related Commands

- `crypto key generate` — generates the SSH keys.
show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

Syntax

show ip ssh client-pub-keys

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Related Commands

- ip ssh server — configures an SSH server.
- show ip ssh client-pub-keys — displays the client-public keys.
show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

Syntax

```
show ip ssh rsa-authentication {my-authorized-keys}
```

Parameters

- **my-authorized-keys**
  Display the RSA authorized keys.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>pre-6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRH1vMc1VZ
d0Sg5GQxRV1yI1JOMeO6N0uYyzyrQMM
4qJAoBwtne0XFb7cHF3V2hcMQa32N+CRCnW/
zCM1nCf0+qVTS1oofsea5r09kS0xT0CNfH3XZ3NuGCq90v33m9+
U9tMw5i8v8AVxdH4x4km3c3t5Jvc=
freedom@poclab4
```

Dell#

**Related Commands**

- `ip ssh rsa-authentication (Config)` — configures the RSA authorized keys.

---

**ssh**

Open an SSH connection specifying the hostname, username, encryption cipher, HMAC algorithm, port number, and version of the SSH client.

**Syntax**

```
ssh [vrf vrf-name] {hostname | ipv4 address | ipv6 address} [-c encryption cipher | -l username | -m HMAC algorithm | -p port-number | -v {1 | 2}]
```

**Parameters**

- `vrf vrf-name` (OPTIONAL) Enter the keyword vrf and then the name of the VRF to specify the VRF used with the SSH session.

  **NOTE:** The VRF configured using this command has a higher precedence than the VRF configured using the `ip ssh vrf vrf-name` command. If you do not configure a VRF using this command, then the SSH client uses the configured VRF (if any). If there is a mismatch between VRFs that are configured using the `ip ssh source-interface` command and the `ssh vrf vrf-name` command, then an error is reported.

- `hostname` (OPTIONAL) Enter the IP address or the host name of the remote device.

- `vrf instance` (OPTIONAL) E-Series Only: Enter the keyword vrf then the VRF Instance name to open an SSH connection to that instance.

- `ipv4 address` (OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.

- `ipv6-address prefix-length` (OPTIONAL) Enter the IPv6 address in the x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

  **NOTE:** The :: notation specifies successive hexadecimal fields of zeros.

- `-c encryption cipher` (OPTIONAL) Enable the "FIPS mode enable", this mode will support only v2 client.
"no fips mode enable"(disable) will support v1 & v2 client. This comment is applicable for both ciphers & HMAC algorithms:

- **3des-cbc**: Force ssh to use 3des-cbc encryption cipher.
- **aes128-cbc**: Force ssh to use aes128-cbc encryption cipher
- **aes192-cbc**: Force ssh to use aes192-cbc encryption cipher
- **aes256-cbc**: Force ssh to use aes256-cbc encryption cipher
- **aes128-ctr**: Force ssh to use aes128-ctr encryption cipher
- **aes192-ctr**: Force ssh to use aes192-ctr encryption cipher
- **aes256-ctr**: Force ssh to use aes256-ctr encryption cipher

- **username** (OPTIONAL) Enter the keyword -l then the user name used in this SSH session. The default is the user name of the user associated with the terminal.

- **m HMAC algorithm** Enter one of the following HMAC algorithms to use. (For v2 clients only):
  "no fips mode enable"(disable) will support v1 & v2 client.

- **hmac-md5**: Force ssh to use hmac-md5 HMAC algorithm.
- **hmac-md5-96**: Force ssh to use hmac-md5-96 HMAC algorithm.
- **hmac-sha1**: Force ssh to use hmac-sha1 HMAC algorithm.
- **hmac-sha1-96**: Force ssh to use hmac-sha1-96 HMAC algorithm.
- **hmac-sha2-256**: Force ssh to use hmac-sha2-256 HMAC algorithm.

- **p port-number** (OPTIONAL) Enter the keyword -p then the port number. The range is from 1 to 65535. The default is 22.

- **v (1 | 2)** (OPTIONAL) Enter the keyword -v then the SSH version 1 or 2. The default is the version from the protocol negotiation.

**Defaults**
As shown in the Parameters section.

**Command Modes**
EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Removed the support for hmac-sha2-256-96 algorithm.
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Added support for the following ciphers and HMAC algorithms on the Z9000, S6000, S4820T, S4820T. S6000-ON.
- **aes128-cbc**
- **aes192-cbc**
- **aes256-cbc**
- **aes128-ctr**
- **aes192-ctr**
- **aes256-ctr**
Secure DHCP Commands

DHCP as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

**clear ip dhcp snooping**

Clear the DHCP binding table.

**Syntax**

```
clear ip dhcp snooping binding
```

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000–ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.8.1.0 | Introduced on the C-Series and S-Series.

Related Commands
- `show ip dhcp snooping` — display the contents of the DHCP binding table.

**ip dhcp relay**

Enable Option 82.

**Syntax**

```
ip dhcp relay information-option [trust-downstream | vrf]
```

**Parameters**

- `trust-downstream` Configure the system to trust Option 82 when it is received from the previous-hop router.
- `vrf` Enter the keyword vrf to include VRF related information in the Option 82. This configuration enables the relay agent to include VRF related information when it forwards the broadcasts from client to DHCP server.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
ip dhcp snooping

Enable DHCP Snooping globally.

Syntax

[no] ip dhcp snooping

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000--ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the C-Series and S-Series.

Usage Information

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP Snooping, the binding table is deleted and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Related Commands

- ip dhcp snooping vlan — enable DHCP Snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Syntax

[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number

Parameters

mac 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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.

slot/port

Enter the slot and port number of the interface.

lease time

Enter the keyword lease then the amount of time the IP address is leased. The range is from 1 to 4294967295.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000--ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.5.1.0 Added support for 4-port 40G line cards.
8.3.7.0 Introduced on the S4810.
7.8.1.0 Introduced on the C-Series and S-Series.

Related Commands

- show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping database

Delay writing the binding table for a specified time.

Syntax

ip dhcp snooping database write-delay minutes

Parameters

minutes The range is from 5 to 21600.

Defaults

none
ip dhcp snooping database renew

Renew the binding table.

Syntax
ip dhcp snooping database renew

Defaults
none

Command Modes
  • EXEC
  • EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>
**ip dhcp snooping trust**

Configure an interface as trusted.

**Syntax**

```
[no] ip dhcp snooping trust
```

**Defaults**

Untrusted

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**ip dhcp source-address-validation**

Enable IP source guard.

**Syntax**

```
[no] ip dhcp source-address-validation
```

**Defaults**

Disabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
</tbody>
</table>
### 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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**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` — configure an interface as trusted.

### show ip dhcp snooping

Display the contents of the DHCP binding table.

**Syntax**

```
show ip dhcp snooping binding
```

**Defaults**

none
Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- clear ip dhcp snooping — clear the contents of the DHCP binding table.

Role-Based Access Control Commands

With Role-Based Access Control (RBAC), access and authorization is controlled based on a user’s role. Users are granted permissions based on their user roles, not on their individual user ID. User roles are created for job functions and through those roles they acquire the permissions to perform their associated job function.

This section describes the syntax and usage of RBAC-specific commands. You can find information on other related security commands in this chapter:

- aaa accounting
- aaa authentication login
- aaa authorization commands
- authorization
- show accounting
- show users
- username

**aaa authorization role-only**

Configure authentication to use the user’s role only when determining if access to commands is permitted.

**Syntax**

```
aaa authorization role-only
```

To return to the default setting, use the no aaa authentication role-only command.
Parameters

**name**

Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).

**inherit existing-role-name**

Enter the *inherit* keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
</tbody>
</table>

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

**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 Dell Networking OS. The range is from 0 to 15.

**Defaults**

15

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series</td>
<td>Original command.</td>
</tr>
</tbody>
</table>

**Usage Information**

Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the `enable password` command to configure a password for the enable command at a specific privilege level. If no privilege level is specified, the default is privilege level 15.

NOTE: If you are authorized for the EXEC Privilege mode by your role, you do not need to enter an enable password.

**Related Commands**

- `enable password` — configures a password for the enable command and to access a privilege level.

**role**

Changes command permissions for roles.

**Syntax**

```plaintext
role mode [{addrole | deleterole} role-name] [reset] command
```

To delete access to a command, use the `no role mode role-name` command.

**Parameters**

- `mode` Enter one of the following keywords as the mode for which you are controlling access:
  - configure for CONFIGURATION mode
  - exec for EXEC mode
  - interface for INTERFACE modes
  - line for LINE mode
  - route-map for Route-map mode
  - router for Router mode
addrole

Enter the keyword addrole to add permission to the command. You cannot add or delete rights for the sysadmin role.

deleterole

Enter the keyword deleterole to remove access to the command. You cannot add or delete rights for the sysadmin role.

role-name

Enter a text string for the name of the user role up to 63 characters. These are 3 system defined roles you can modify: secadmin, netadmin, and netoperator.

reset

Enter the keyword reset to reset all roles back to default for that command.

command

Enter the command’s keywords to assign the command to a certain access level. You can enter one or more keywords.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(1.0) Introduced on the Z9100-ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.5(0.0) Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Related Commands

• userrole — creates user roles.

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
show userroles

Display information on all defined user roles.

Syntax

show userroles

Example

Dell# show userroles
Role          Inheritance  Modes
netoperator                Exec
netadmin                   Exec Config Interface Line Router IP
                          Route-map Protocol MAC
secadmin                   Exec Config
sysadmin                   Exec Config Interface Line Router IP
                          Route-map Protocol MAC
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
netoperator
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** — create user roles.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9000, S6000, S4820T, S4810, MXL</td>
</tr>
</tbody>
</table>
### Example

```plaintext
Dell# show userroles
Role   Inheritance    Modes
netoperator Exec
netadmin   Exec Config Interface Line Router IP Route-map Protocol MAC
secadmin   Exec Config
sysadmin   Exec Config Interface Line Router IP Route-map Protocol MAC
netoperator
netadmin   Exec Config Interface Line Router IP Route-map Protocol MAC
```
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.

```
role mode { { { addrole | deleterole } role-name } | reset } command – Modifies (adds or deletes) command permissions for newly created user roles and system defined roles.
```

**Related Commands**

- `role mode { { (addrole | deleterole) role-name } | reset } command` — modifies (adds or deletes) command permissions for newly created user roles and system defined roles.
Service Provider Bridging

Service provider bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the Dell Networking OS Configuration Guide Service Provider Bridging section.

This section includes command line information (CLI) for the Dell Networking OS Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

Dell Networking OS supports L2PT on Dell Networking OS.

For more information, 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 (BFDU) 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

debbug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]

To disable debugging, use the no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value] command.

Parameters

- interface
  - Enter one of the following interfaces and the interface information:
    - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.

**in | out | both** Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.

**vlan vlan-id** Enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

**count value** Enter the keyword `count` then the number of debug outputs. The range is from 1 to 100.

**Defaults** Debug disabled.

**Command Modes** EXEC Privilege

**Command History** This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series, and E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**protocol-tunnel**

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

**Syntax**

```
protocol-tunnel {rate-limit rate| stp}
```

To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

**Parameters**

- `rate-limit rate` Enter the keyword `rate-limit` followed by a number for the rate-limit for tunneled packets on the VMAN. The range is from 64 to 320.

- `stp` Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.

**Defaults** none
Command Modes

**CONF-IF-VLAN**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.1</td>
<td>Added support for 802.1X, E-LMI, GMRP, GVRP, LLDP, LACP, MMRP, MVRP, and OAM 802.3ah protocol traffic to the E-Series.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series, E-Series, and E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example

Dell# conf
Dell(conf)# interface vlan 2
Dell(conf-if-vl-2)# vlan-stack compatible
Dell(conf-if-vl-2)# member Gi1/2-3
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**

- `stp` Change the default destination MAC address used for L2PT to another value.

**Defaults**

The default destination MAC is 01:01:e8:00:00:00.

**Command Modes**

**CONFIGURATION**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
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**

```plaintext
protocol-tunnel enable
```

To disable protocol tunneling, use the `no protocol-tunnel enable` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series, and S-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Usage Information**

Dell Networking OS must have the default CAM profile with the default microcode before you enable L2PT.
**protocol-tunnel rate-limit**

Enable traffic rate limiting per box.

**Syntax**

```
protocol-tunnel rate-limit rate
```

To reset the rate limit to the default, use the `no protocol-tunnel rate-limit rate` command.

**Parameters**

- `rate` Enter the rate in frames per second. The range is from 75 to 3000. The default is 75.

**Defaults**

75 frames per second.

**Command Modes**

CONF-IF-VLAN-STACK

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series and E-Series. Maximum rate limit on E-Series reduced from 4000 to 3000.</td>
</tr>
<tr>
<td>7.41.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

**Example**

```
Dell(conf-if-vl-2)# vlan-stack compatible
Dell(conf-if-vl-2-stack)#protocol-tunnel rate-limit 100 <<<<<<<< VLAN stack mode
Dell(conf-if-vl-2-stack)#show config
!
interface Vlan 2
  no ip address
  mtu 1000
  vlan-stack compatible
  protocol-tunnel rate-limit 100
  shutdown
```

**Related Commands**

- `show protocol-tunnel` — displays tunneling information for all VLANs.
- `show running-config` — displays the current configuration.
show protocol-tunnel

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

Syntax
show protocol-tunnel [vlan vlan-id]

Parameters
- **vlan vlan-id** (OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.

Defaults
none

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the C-Series, and E-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced</td>
</tr>
</tbody>
</table>

Example
```
Dell# show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN Protocols Interface
1000 STP, PVST Gi 5/7,Gi 5/6
1001 LLDP, GVRP Gi 5/7,Gi 5/6
1002 MMRP, MVRP Gi 5/7,Gi 5/6
1003 LACP, DOT1X Gi 5/7,Gi 5/6
1004 OAM, PAUSE Gi 5/7,Gi 5/6
1005 E-LMI Gi 5/7,Gi 5/6
```

Example (Specific VLAN)
```
Dell# show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface Vlan Protocol(s)
Gi1/2 2 STP, PVST
```

Related Commands
- `show running-config` — displays the current configuration.
The Dell Networking OS supports sFlow commands.
The Dell Networking OS sFlow monitoring system includes an sFlow Agent and an sFlow Collector.

- The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector.
- The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

**Important Points to Remember**

- Dell Networking recommends that the sFlow Collector be connected to the Dell Networking chassis through a line card port rather than the route processor module (RPM) Management Ethernet port.
- Dell Networking OS exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to many exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- The source virtual local area network (VLAN) field in the extended switch element is not packed if there is a routed packet.
- The destination VLAN field in the extended switch element is not packed if there is a multicast packet.
- The sFlow sampling functionality is supported only for egress traffic and not for ingress traffic.
- The maximum number of packets that can be sampled and processed per second is:
  - 7500 packets when no extended information packing is enabled.
  - 7500 packets when only extended-switch information packing is enabled (see `sflow extended-switch enable`).

**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
sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

Syntax

sflow collector {ip-address | ipv6-address} agent-addr {ip-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number] [vrf management]

To delete a configured collector, use the no sflow collector {ip-address | ipv6-address} agent-addr {ipv4-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number] [vrf management] command.

Parameters

- **sflow collector ip-address | ipv6-address**: Enter the IP address of the collector in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6.
  - **NOTE**: The :: notation specifies successive hexadecimal fields of zeros.

- **agent-addr ip-address | ipv6-address**: Enter the keyword agent-addr followed by the sFlow agent IP address in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6.
  - **NOTE**: The :: notation specifies successive hexadecimal fields of zeros.

- **number**: (OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is from 0 to 65535. The default is 6343.

- **max-datagram-size number**: (OPTIONAL) Enter the keyword max-datagram-size then the size number in bytes. The range is from 400 to 1500. The default is 1400.

- **vrf management**: (OPTIONAL) Enter the keyword vrf followed by the keyword management to configure the collector device corresponding to the default VRF and the management VRF respectively.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.4(2.3)</td>
<td>Added support for IPv6 sFlow collectors and agents on the E-series, C-Series, and S-Series.</td>
</tr>
</tbody>
</table>
### sFlow enable (Global)

Enable sFlow globally.

**Syntax**

```
sflow enable
```

To disable sFlow, use the `no sflow enable` command.

**Defaults**

Disabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>

---

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.

In sFlow, the agent address is a single invariant IPv4 or IPv6 address used to identify the agent to the collector. It is usually assigned the address of a loopback interface on the agent, which provides invariance. The agent address is carried as a field in the payload of the sFlow packets.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, Dell Networking OS returns the corresponding configured agent IP in the MIB requests. Dell Networking OS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, Dell Networking OS generates the following error: `%Error: Different agent-addr attempted for an existing collector.`

Example

```
Dell(conf)# sflow collector 10.1.1.25 agent-addr 10.1.1.10 vrf management
```

---

## Version Description

- **8.4.1.1**: Added support for IPv6 sFlow collectors and agents on the E-series.
- **8.3.7.0**: Introduced on the S4810.
- **8.2.1.0**: Introduced S-Series Stacking.
- **8.1.1.0**: Introduced on the E-Series.
- **7.7.1.0**: Introduced on the S-Series.
- **7.6.1.0**: Introduced on the C-Series.
- **6.5.1.0**: Expanded the `no` form of the command to mirror the syntax used to configure.
- **6.2.1.1**: Introduced on the E-Series.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced S-Series Stacking.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.

**Related Commands**

- `sflow enable (Interface)` — enable sFlow on interfaces.

---

**sflow ingress-enable**

Enable sFlow ingress on interfaces.

**Syntax**

```
sflow ingress-enable
```

To disable sFlow, use the `no sflow ingress enable` command.

**Defaults**

Disabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S-Series, Z-Series, and MxL switch.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

**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)` — turn sFlow globally.
sflow extended-switch enable

Enable packing information on a switch only.

Syntax

sflow extended-switch enable

To disable packing information, use the no sflow extended-switch [enable] command.

Parameters

enable Enter the keyword enable to enable global extended information.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on S-Series Stacking.
8.1.1.0 Introduced on the E-Series.
7.7.1.0 Introduced on the S-Series.
7.6.1.0 Introduced on the C-Series.
7.4.1.0 Introduced on the E-Series.

Usage Information

Dell Networking OS enhances the sflow implementation for real time traffic analysis on the E-Series to provide extended gateway information in cases where the destination IP addresses are learned by different routing protocols and for cases where the destination is reachable over ECMP.

Related Commands

- show sflow — displays the sFlow configuration.

sflow max-header-size extended

Set the maximum header size of a packet to 256 bytes.

Syntax

sflow max-header-size extended
To reset the maximum header size of a packet, use the `no sflow max-header-size extended` command.

**Parameters**
- **extended**
  
Enter the keyword `extended` to copy 256 bytes from the sample packets to sFlow datagram.

**Defaults**
- **128 bytes**

**Command Modes**
- **CONFIGURATION**
- **INTERFACE**

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S Series and Z Series switches.</td>
</tr>
</tbody>
</table>

**Example**
```
Dell(conf)# sflow max-header-size extended
```

### sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

**Syntax**
```
sflow polling-interval interval value
```

To return to the default, use the `no sflow polling-interval interval` command.

**Parameters**
- **interval value**
  
Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is **20 seconds**.

**Defaults**
- **20 seconds**

**Command Modes**
- **CONFIGURATION**

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
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.

**Usage Information**

**Related Commands**

- `sflow polling-interval (Interface)` — sets the polling interval for an interface.

**sflow polling-interval (Interface)**

Set the sFlow polling interval at an interface (overrides the global-level setting.)

**Syntax**

```
 sflow polling-interval interval value
```

To return to the default, use the `no sflow polling-interval interval value` command.

**Parameters**

- `interval value` Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is the current global default counter polling interval.

**Defaults**

The same value as the current global default counter polling interval.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on S-Series Stacking.</td>
</tr>
<tr>
<td>8.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
8.2.1.0 | Introduced on S-Series Stacking.
8.1.1.0 | Introduced on the E-Series.
7.7.1.0 | Introduced on the S-Series.
7.6.1.0 | Introduced on the C-Series.
7.4.1.0 | Introduced on the E-Series.

Usage Information
This command sets the counter polling interval for an interface.

Related Commands
- `sflow polling-interval (Global)` — globally sets the polling interval.

**sflow sample-rate (Global)**

Change the global default sampling rate.

**Syntax**

```
sflow sample-rate value
```

To return to the default sampling rate, use the `no sflow sample-rate` command.

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Enter the sampling rate value. For the C-Series and S-Series, the range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, and so on. The default is <strong>32768 packets</strong>.</td>
</tr>
</tbody>
</table>

**Defaults**

**32768 packets**

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

**Version** | **Description**
--- | ---
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
8.2.1.0 | Introduced on S-Series Stacking.
8.1.1.0 | Introduced on the E-Series.
7.7.1.0 | Introduced on the S-Series.
7.6.1.0 | Introduced on the C-Series.
Usage Information
Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.

Related Commands
- sflow sample-rate (Interface) — changes the interface sampling rate.

sflow sample-rate (Interface)
Change the interface default sampling rate.

Syntax
sflow sample-rate value
To return to the default sampling rate, use the no sflow sample-rate command.

Parameters
value
Enter the sampling rate value. For the C-Series and S-Series, the range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, etc. The default is 32768 packets.

Defaults
The Global default sampling.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
8.2.1.0 Introduced on S-Series Stacking.
8.1.1.0 Introduced on the E-Series.
7.7.1.0 Introduced on the E-Series.
7.6.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Usage Information
This command changes the sampling rate for an interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the
command generates an error message with the previous and next power-of-2 value. Select one of these two
number and re-enter the command.

Related Commands

• `sflow sample-rate (Global)` — changes the sampling rate globally.

**show sflow**

Display the current sFlow configuration.

**Syntax**

```
show sflow [interface]
```

**Parameters**

- **interface** (OPTIONAL) Enter the following keywords and slot/port or number information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For the Management interface on the, enter the keyword ManagementEthernet then the slot/port information.
  - For a port-channel interface, enter the keywords port-channel then the port-channel ID.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on S-Series Stacking.</td>
</tr>
<tr>
<td>8.1(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
6.2.1.1 | Introduced on the E-Series.

Usage Information
The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example always displays a value of zero.

Example
```
Dell#show sflow
sFlow services are enabled
Egress Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collectors configured
Collector IP addr: 100.1.1.1, Agent IP addr: 1.1.1.2, UDP port: 6343 VRF: Default
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected

stack-unit 1 Port set 1
    Gi 1/1: configured rate 16384, actual rate 16384 <<< sampling rate based on line speed if global sampling rate is default
Dell#
```
Simple Network Management Protocol (SNMP) and Syslog

This section contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog. Both features are supported on Dell Networking OS.

Topics:
- SNMP Commands
- Syslog Commands

SNMP Commands

The following SNMP commands are available in the Dell Networking OS.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. Dell Networking OS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. Dell Networking OS sends SNMP traps, which are messages informing an SNMP management system about the network. Dell Networking OS supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout — greater than 3 seconds.
  - SNMP Retry count — greater than 2 seconds.
- If you want to query an E-Series switch using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on a non-management port on the switch.
- If you want to send SNMP v1/v2/v3 traps from an E-Series using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

show snmp

Display the status of SNMP network elements.

Syntax

```
show snmp
```

Command Modes

- EXEC
- EXEC Privilege
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.
- **9.8(1.0)** Introduced on the Z9100–ON.
- **9.8(0.0P5)** Introduced on the S4048-ON.
- **9.8(0.0P2)** Introduced on the S3048-ON.
- **9.7(0.0)** Introduced on the S6000-ON.
- **9.2(1.0)** Introduced on the Z9500.
- **9.0.2.0** Introduced on the S6000.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.7.0** Introduced on the S4810.
- **7.6.1.0** Introduced on the S-Series.
- **7.5.1.0** Introduced on the C-Series.

**E-Series legacy command**

### Example

```
Dell# show snmp
32685 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
96988 Number of requested variables
  0 Number of altered variables
968 Get-request PDUs
31681 Get-next PDUs
968 Get-next PDUs
0 Set-request PDUs
61727 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  9 No such name errors
  0 Bad values errors
  0 General errors
32649 Response PDUs
29078 Trap PDUs
Dell#
```

### Related Commands

- `snmp-server community` — enables the SNMP and set community string.

### show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

**Syntax**

```
show snmp engineID
```

**Command Modes**

- EXEC
- EXEC Privilege
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Example

Dell# show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID       IP-addr      Port
80001F88043132333435   172.31.1.3   5009
80001F88043938373635   172.31.1.3   5008
Dell#

Related Commands

- `snmp-server engineID` — configures local and remote SNMP engines on the router.

show snmp group

Display the group name, security model, status, and storage type of each group.

Syntax

```
show snmp group
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
show snmp user

Display the information configured on each SNMP user name.

Syntax

```
show snmp user
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.10(0.0) Introduced on the S6100–ON.
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.
```

Related Commands

- `snmp-server group` — configures an SNMP server group.

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.

```
Dell# show snmp group
groupName: v1v2creadg   security model: v1
readview : v1v2cdefault  writeview: no write view specified
notifyview: v1v2cdefault  context: no context specified
row status: active
Dell#
```
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Example**

Dell#show snmp user
User name: v1v2creadu
Engine ID: 0000178B02000001E80214A8
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None

Dell#

### snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

**Syntax**

```
snmp ifmib ifalias long
```

**Defaults**

Interface description truncated beyond 63 characters.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**Example**

Dell#config!------command run on host connected to switch: ------------------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This
is a port connected to
IF-MIB::ifAlias.134792448 = STRING:

!------command run on Dell Networkingswitch: ---------------!
Dell#snmp ifmib ifalias long

!------command run on server connected to switch: ---------------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This
is a port connected to Router2. This is a port connected to Router2. This is a
port connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
Dell#config

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

Syntax

```
snmp-server community community-name {ro | rw} [ipv6 ipv6-access-list-name
[ipv6 ipv6-access-list-name | access-list-name | security-name name] |
security-name name [ipv6 ipv6-access-list-name | access-list-name | security-
name name] | access-list-name [ipv6 ipv6-access-list-name | access-list-name |
security-name name]]]]
```

To remove access to a community, use the no snmp-server community community-string {ro | rw} [security-name name [access-list-name | ipv6 access-list-name | access-
list-name ipv6 access-list-name]] command.

Parameters

- `community-name`: Enter a text string (up to 20 characters long) to act as a password for SNMP.
- `ro`: Enter the keyword `ro` to specify read-only permission.
- `rw`: Enter the keyword `rw` to specify read-write permission.
- `ipv6 access-list-name`: (Optional) Enter the keyword `ipv6` then an IPv6 ACL name (a string up to 16 characters long).
- `security-name name`: (Optional) Enter the keywords `security-name` then the security name as defined by the community MIB.
- `access-list-name`: (Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0)  Introduced on the S6100–ON.
9.8(1.0)  Introduced on the Z9100–ON.
9.8(0.0P5)  Introduced on the S4048-ON.
9.8(0.0P2)  Introduced on the S3048-ON.
9.7(0.0)  Introduced on the S6000-ON.
9.2(1.0)  Introduced on the Z9500.
### Version

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

The following example configures a community named public that is mapped to the security named guestuser with Read Only (ro) permissions.

```text
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:

- `vlv2creadu` / `vlv2creadg` — maps to a community with ro (read-only) permissions.
- `vlv2cwriteu` / `vlv2cwriteg` — 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

```text
Dell# config
Dell(conf)# snmp-server community public ro
Dell(conf)# snmp-server community guest ro security-name guestuser
Dell(conf)#
```

```text
Dell(conf)# ip access-list standard snmp-ro-acl
Dell(config-standard-nacl)#seq 5 permit host 10.10.10.224
Dell(config-standard-nacl)#seq 10 deny any count
Dell(conf)# snmp-server community guest ro snmp-ro-acl
Dell(conf)#
```

### Related Commands

- `ip access-list standard` — names (or selects) a standard access list to filter based on IP address.
- `ipv6 access-list` — configures an access list based on IPv6 addresses or protocols.
- `show running-config` — displays the current SNMP configuration and defaults.
**snmp-server contact**

Configure contact information for troubleshooting this SNMP node.

**Syntax**

```
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

**Parameters**

- `text` : Enter an alphanumeric text string, up to 55 characters long.

**Defaults**

none

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

---

**snmp-server enable traps**

Enable SNMP traps.

**Syntax**

```
snmp-server enable traps [notification-type] [notification-option]
```

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.

**Parameters**

- `notification-type` : Enter the type of notification from the following list:
  - `bgp` — Notification of changes in the BGP process.
  - `config` — Notification of changes to the startup or running configuration.
- **ecfm** — Notification of changes to ECFM.
- **ecmp** — Enable an ECMP trap to notify of ECMP or link bundle traffic imbalances.
- **envmon** — For Dell Networking device notifications when an environmental threshold is exceeded.
- **isis** — Notification of intermediate service traps.
- **lacp** — Notification of changes.
- **snmp** — Notification of RFC 1157 traps.
- **stp** — Notification of a state change in the spanning tree protocol (RFC 1493).
- **vlt** — Notification of virtual link trunking.
- **vrrp** — Notification of a state change in a VRRP group.
- **xstp** — Notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST +.

**notification-option**

For the **envmon** notification-type, enter one of the following optional parameters:

- cam-utilization
- fan
- supply
- temperature

For the **snmp** notification-type, enter one of the following optional parameters:

- authentication
- coldstart
- linkdown
- linkup
- syslog-reachable
- syslog-unreachable

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.8(0.0)</td>
<td>Added the following two SNMP notification options: syslog-reachable and syslog-unreachable.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
## Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1(0.0)</td>
<td>Added support for copy-config and ECMP traps.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for VRRP traps.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for STP and xSTP traps. Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

Dell Networking OS supports up to 16 SNMP trap receivers.

If you do not configure this command, traps that controlled by this command are not sent. If you do not specify a notification-type and notification-option, all traps are enabled.

### Related Commands

- `snmp-server community` — enables SNMP and sets the community string.

### `snmp-server engineID`

Configure the name for both the local and remote SNMP engines on the router.

**Syntax**

```plaintext
snmp-server engineID [local engineID] [remote ip-address vrf vrf-name udp-port port-number engineID]
```

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address vrf vrf-name udp-port port-number engineID]` command.

**Parameters**

- `local engineID`  
  Enter the keyword `local` followed by the engine ID number that identifies the copy of the SNMP on the local device.

  Format (as specified in RFC 3411): 12 octets.

  - The first four octets are set to the private enterprise number.
  - The remaining eight octets are the MAC address of the chassis.

- `remote ip-address`  
  Enter the keyword `remote` followed by the IP address that identifies the copy of the SNMP on the remote device.

- `vrf vrf-name`  
  Enter the keyword `vrf` followed by the name of the VRF that is used to reach the device. **NOTE:** Use this attribute to specify the VRF that is used by the SNMP engine to reach the device. If no VRF is specified, then the default VRF is used.

- `udp-port port-number engineID`  
  Enter the keywords `udp-port` followed by the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is 162.

**Defaults**

As above.
Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

Changing the value of the SNMP Engine ID has important side effects. A user’s password (entered on the command line) is converted to a message digest algorithm (MD5) or secure hash algorithm (SHA) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users is invalid and the users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands

- `show snmp engineID` — displays the SNMP engine and all the remote engines that are configured on the router.
- `show running-config snmp` — displays the SNMP running configuration.

**snmp-server group**

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

**Syntax**

```
snmp-server group [group_name {v1 | v2c | 3 [auth | noauth | priv]}] [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a specified group, use the **no snmp-server group [group_name {v1 | v2c | 3 [auth | noauth | priv]}] [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]** command.
**Parameters**

- **group_name**: Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults):
  - `v1v2creadg` — maps to a community/security-name with `ro` permissions.
  - `v1v2cwriteg` — maps to a community/security-name `rw` permissions.

- **1 | 2c | 3**: (OPTIONAL) Enter the security model version number (1, 2c, or 3):
  - 1 is the least secure version.
  - 3 is the most secure of the security modes.
  - 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

  The default is 1.

- **auth** (OPTIONAL) Enter the keyword auth to specify authentication of a packet without encryption.

- **noauth** (OPTIONAL) Enter the keyword noauth to specify no authentication of a packet.

- **priv** (OPTIONAL) Enter the keyword priv to specify both authentication and then scrambling of the packet.

- **read name** (OPTIONAL) Enter the keyword read then a name (a string of up to 20 characters long) as the read view name. The default is **GlobalView** and is assumed to be every object belonging to the internet (1.3.6.1) OID space.

- **write name** (OPTIONAL) Enter the keyword write then a name (a string of up to 20 characters long) as the write view name.

- **notify name** (OPTIONAL) Enter the keyword notify then a name (a string of up to 20 characters long) as the notify view name.

- **access access-list-name** (Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

- **ipv6 access-list-name** (Optional) Enter the keyword ipv6 then the IPv6 access list name (a string up to 16 characters long).

- **access-list-name ipv6 access-list-name** (Optional) Enter both an IPv4 and IPv6 access list name.

**Defaults**

As above.

**Command Modes**

- **CONFIGURATION**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
</tbody>
</table>
### snmp-server group

Configure the recipient of an SNMP trap operation.

**Syntax**

```plaintext
snmp-server host ip-address | ipv6-address [vrf vrf-name] traps | informs [version 1 | 2c | 3] [auth | no auth | priv] [community-string] [udp-port port-number] [notification-type]
```

To remove the SNMP host, use the `no snmp-server host ip-address | ipv6-address [vrf vrf-name] traps | informs [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Enter the keyword host then the IP address of the host (configurable hosts is limited to 16).</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>Enter the keyword host then the IPv6 address of the host in the x:x:x:x format.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>Enter the keyword vrf and then the name of the VRF that the SNMP server uses to connect to the host.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
Dell# conf
Dell(conf)# snmp-server group harig 3 priv read rview
Dell#
```

**Related Commands**

- `show snmp group` — displays the group name, security model, view status, and storage type of each group.
- `show running-config` — displays the SNMP running configuration.

**Usage Information**

The following example specifies the group named `harig` as a version 3 user requiring both authentication and encryption and read access limited to the read named `rview`.

```plaintext
NOTE: The number of configurable groups is limited to 16 groups.
```

### snmp-server host

Configure the recipient of an SNMP trap operation.

**Syntax**

```plaintext
snmp-server host ip-address | ipv6-address [vrf vrf-name] traps | informs [version 1 | 2c | 3] [auth | no auth | priv] [community-string] [udp-port port-number] [notification-type]
```

To remove the SNMP host, use the `no snmp-server host ip-address | ipv6-address [vrf vrf-name] traps | informs [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

**Parameters**

- `ip-address`
- `ipv6-address`
- `vrf vrf-name`

**Example**

```plaintext
Dell# conf
Dell(conf)# snmp-server host harig 3 priv read rview
Dell#
```

**Related Commands**

- `show snmp group` — displays the group name, security model, view status, and storage type of each group.
- `show running-config` — displays the SNMP running configuration.
NOTE: You can use this attribute to inform the SNMP engine about the vrf instance to be used to reach the corresponding remote host to send Trap or Inform message. If no VRF is specified, then the default VRF is used.

traps (OPTIONAL) Enter the keyword traps to send trap notifications to the specified host. The default is traps.

informs (OPTIONAL) Enter the keyword informs to send inform notifications to the specified host. The default is traps.

version 1 | 2c | 3 (OPTIONAL) Enter the keyword version to specify the security model then the security model version number 1, 2c, or 3:

- Version 1 is the least secure version.
- Version 3 is the most secure of the security modes.
- Version 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

The default is version 1.

auth (OPTIONAL) Enter the keyword auth to specify authentication of a packet without encryption.

noauth (OPTIONAL) Enter the keyword noauth to specify no authentication of a packet.

priv (OPTIONAL) Enter the keyword priv to specify both authentication and then scrambling of the packet.

community-string Enter a text string (up to 20 characters long) as the name of the SNMP community.

NOTE: For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking OS recommends setting the community string using the snmp-server community command before executing this command. For version 3 security model, this string is the USM user security name.

udp-port port-number (OPTIONAL) Enter the keywords udp-port followed by the port number of the remote host to use. The range is from 0 to 65535. The default is 162.

notification-type (OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host:

- bgp — Enable BGP state change traps.
- ecfm — Enable ECFM state change traps.
- entity — Enable entity change traps.
- envmon — Enable SNMP environmental monitor traps.
- eoam — Enable EOAM state change traps
- ets — Enable ets traps
- fips — Enable FIP Snooping state change traps
- lacp — Enable LACP state change traps.
- isis — Enable ISIS adjacency change traps
- pfc — Enable pfc traps
- smtp — Enable SNMP trap
- stp — Enable 802.1d state change traps
- vlt — Enable VLT traps
- vrrp — Enable VRRP state change traps
- `xstp` — Enable 802.1s, 802.1w, and PVST+ state change traps

The default is all trap types are sent to host.

**Defaults**
As above.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Added support for config and ecmp traps.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for VRRP traps.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Added support for STP and xSTP notification types.</td>
</tr>
<tr>
<td></td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Usage Information**
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 enable` command, no notifications are sent.

In order to enable multiple hosts, issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command will be in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command replaces the first command.

The `snmp-server host` command is used with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable command and the snmp-server host command for that host must be enabled.
NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group for this user with access rights.
4. Enable traps.
5. Configure a host to receive informs.

Related Commands

- `snmp-server enable traps` — enables SNMP traps.
- `snmp-server community` — configures a new community SNMPv1 or SNMPv2c.

**snmp-server location**

Configure the location of the SNMP server.

```
Syntax
snmp-server location text

To delete the SNMP location, use the no snmp-server location command.
```

**Parameters**

- `text`  
  Enter an alpha-numeric text string, up to 55 characters long.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>
### snmp-server packetsize

Set the largest SNMP packet size permitted. When the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize` global configuration command.

**Syntax**

```plaintext
snmp-server packetsize byte-count
```

**Parameters**

- `byte-count`
  - Enter one of the following values: 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.

**Defaults**

- 8

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

### snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

**Syntax**

```plaintext
snmp-server trap-source interface
```

To disable sending traps out a specific interface, use the `no snmp trap-source` command.
**Parameters**

Enter the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
- For a port channel interface, enter the keywords port-channel then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

**Defaults**

The IP address assigned to the management interface is the default.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**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 vrf vrf-name udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv {des56 | aes128} priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv {des56 | aes128} priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]` command.

**Parameters**

- **name**
  
Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.

- **group_name**
  
Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults):
  
  - `v1v2creadu` — maps to a community with `ro` permissions.
  - `1v2cwriteu` — maps to a community `rw` permissions.

- **remote ip-address**
  
Enter the keywords `udp-port` then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is `162`.

- **vrf vrf-name**
  
Enter the keywords `vrf` and then the name of the VRF this is used to connect to the SNMP server.

  **NOTE:** Use this attribute to specify a VRF name that is used to connect to the remote host. If no VRF is specified, then the default VRF is used.

- **udp-port port-number**
  
Enter the keywords `udp-port` then the UD (User Datagram Protocol) port number on the remote device. The range is from 0 to 65535. The default is `162`.

- **1 | 2c | 3**
  
  (OPTIONAL) Enter the security model version number (1, 2c, or 3):
  
  - 1 is the least secure version.
  - 3 is the most secure of the security modes.
  - 2c allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed.

  The default is `1`.

- **encrypted**
  
  (OPTIONAL) Enter the keyword `encrypted` to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).

- **auth**
  
  (OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.

- **md5 | sha**
  
  (OPTIONAL) Enter the keyword `md5` or `sha` to designate the authentication level.

  - `md5` — Message Digest Algorithm
  - `sha` — Secure Hash Algorithm
auth-password

(Optional) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host. Minimum: eight characters long.

priv

(Optional) Enter the keywords priv to initiate a privacy authentication level setting.

des56 | aes128

(Optional) Enter the keyword des56 or aes128 to specify the encryption mode.

  • aes128 — Use 128 bit AES algorithm in CFB mode for encryption.
  • des56 — Use 56 bit DES algorithm in CBC mode for encryption.

priv password

(Optional) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent. Minimum: eight characters long.

access access-list-name

(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).

ipv6 access-list-name

(Optional) Enter the keyword ipv6 then the IPv6 access list name (a string up to 16 characters long).

access-list-name

(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults

As above.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.6.(0.0) Added aes 128 encryption algorithm parameter.
9.4.(0.0) Added support for VRF.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.

Usage Information

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP. TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

No default values exist for authentication or privacy algorithms and no default password exists. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an
encrypted cypher-text password. In either case, the password is stored in the configuration in an encrypted form and displayed as encrypted in the `show running-config` command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an Example of how to specify the command with an encrypted string.

```
NOTE: The number of configurable users is limited to 16.
```

**Example**

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5 9fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3e42804fe80e3ba8763d
```

**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)# 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)# 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 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 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

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Added support for the AES128-CFB encryption algorithm on the S4820T, S4810, S6000 and Z-Series platforms</td>
</tr>
</tbody>
</table>

**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 version 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**
- `view-name` Enter the name of the view (not to exceed 20 characters).
- `oid-tree` Enter the OID sub tree for the view (not to exceed 20 characters).
- `included` *(OPTIONAL)* Enter the keyword `included` to include the MIB family in the view.
(OPTIONAL) Enter the keyword `excluded` to exclude the MIB family in the view.

Defaults

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information

The `oid-tree` variable is a full sub-tree starting from 1.3.6 and cannot specify the name of a sub-tree or a MIB. The following Example configures a view named `rview` that allows access to all objects under 1.3.6.1.

Example

```
Dell# conf
Dell#(conf) snmp-server view rview 1.3.6.1 included
```

Related Commands

- `show running-config snmp` — displays the SNMP running configuration.

**snmp-server vrf**

Configures an SNMP agent to bind to a specific VRF.

**Syntax**

```
snmp-server vrf vrf-name
```

To undo the SNMP agent configuration, use the `no snmp-server vrf vrf-name` command.

**Parameters**

- `vrf vrf-name` Enter the keyword `vrf` and then the name of the VRF to associate an SNMP agent with that VRF.

**Defaults**

Not Enabled.

**Command Modes**

CONFIGURATION
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.
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.4(0.0) | Introduced on the S-Series and Z9000.

**Usage Information**

Use this command to bind an SNMP agent to a VRF. The SNMP agent processes the requests from the interfaces that belong to the specified VRF. If no VRF is specified, then the default VRF is used.

**Related Commands**

- `show snmp user` — display the information configured on each SNMP user name.

### snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

**Syntax**

```
snmp trap link-status
```

To disable sending link trap messages, use the `no snmp trap link-status` command.

**Defaults**

Enabled.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
---|---
9.10(0.0) | Introduced on the S6100–ON.
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
9.2(0.0) | Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

#### Usage Information

If the interface is expected to flap during normal usage, you could disable this command.

## Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

### clear logging

Clear the messages in the logging buffer.

**Syntax**

```
clear logging
```

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

#### E-Series legacy command
Related Commands
- `show logging` — display logging settings and system messages in the internal buffer.

clear logging auditlog

Clears audit log.

Syntax
```
clear logging auditlog
```

Defaults
None

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the MXL.</td>
</tr>
</tbody>
</table>

Example
```
Dell(conf)# clear logging auditlog
```

Related Commands
- `show logging auditlog` — display the audit log.

default logging buffered

Return to the default setting for messages logged to the internal buffer.

Syntax
default logging buffered

Defaults
```
size = 40960; level = 7 or debugging
```

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>
default logging console

Return the default settings for messages logged to the console.

Syntax

default logging console

Defaults

level = 7 or debugging

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Related Commands

- logging console — set the logging console parameters.

Version Description

9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
E-Series legacy command

Related Commands

- logging buffered — set the logging buffered parameters.
default logging monitor

Return to the default settings for messages logged to the terminal.

Syntax

```
default logging monitor
```

Defaults

```
level = 7 or debugging
```

Command Modes

```
CONFIGURATION
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Related Commands

- `logging monitor` — set the logging monitor parameters.
- `terminal monitor` — send system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

Syntax

```
default logging trap
```

Defaults

```
level = 6 or informational
```

Command Modes

```
CONFIGURATION
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Related Commands

- logging trap — limit messages logged to the Syslog servers based on severity.

**logging**

Configure an IP address or host name of a Syslog server where logging messages are sent. Multiple logging servers of both IPv4 and/or IPv6 can be configured.

**Syntax**

```
logging {ip-address | ipv6-address | hostname} {{udp {port}} | {tcp {port}}} |
[vrf vrf-name]
```

To disable logging, use the no logging command.

**Parameters**

- **ip-address**: Enter the IPv4 address in dotted decimal format.
- **ipv6-address**: Enter the IPv6 address in the x:x:x:x::X format.

  | NOTE: The :: notation specifies successive hexadecimal fields of zeros.

- **hostname**: Enter the name of a host already configured and recognized by the switch.
- **udp**: Enter the keyword udp to enable transmission of log message over UDP followed by port number. The default port is 514.
- **tcp**: Enter the keyword tcp to enable transmission of log message over TCP followed by port number.
- **vrf vrf-name**: (Optional) Enter the keyword vrf and then the name of the VRF to enable the logging process in VRF mode.

  | NOTE: Use this attribute to specify the VRF that is used to contact the host. By default, the default VRF is used.
Defaults
Disabled.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Added udp and tcp keywords for the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added udp and tcp keywords for the S4810, S4820T, S6000, Z9000, and MXL.</td>
</tr>
<tr>
<td>9.4,(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Added support for IPv6.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

Usage Information
Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Related Commands
- logging on — enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.
- logging trap — enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Syntax
logging buffered [level] [size]

To return to the default values, use the default logging buffered command.

To disable logging stored to an internal buffer, use the no logging buffered command.
Parameters

- **level** (OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 7 or debugging.

- **size** (OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is from 40960 to 524288. The default is 40960 bytes.

Defaults

- level = 7
- size = 40960 bytes

Command Modes

- **CONFIGURATION**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

- clear logging — clears the logging buffer.
- default logging buffered — returns the logging buffered parameters to the default setting.
- show logging — displays the logging setting and system messages in the internal buffer.

**logging console**

Specify which messages are logged to the console.

**Syntax**

```
logging console [level]
```

To return to the default values, use the default logging console command.
To disable logging to the console, use the `no logging console` command.

**Parameters**

- `level` (OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 7 or `debugging`.

**Defaults**

- `level = 7; size = debugging`

**Command Modes**

- `CONFIGURATION`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

**Related Commands**

- `clear logging` — clears the logging buffer.
- `default logging console` — returns the logging console parameters to the default setting.
- `show logging` — displays the logging setting and system messages in the internal buffer.

**logging extended**

Logs security and audit events to a system log server.

**Syntax**

```
logging extended
```

**Defaults**

none

**Command Modes**

- `CONFIGURATION`
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL.</td>
</tr>
</tbody>
</table>

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** — display the audit log.
- **clear logging auditlog** — clear the audit log.

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

**Syntax**

logging facility [facility-type]

To return to the default values, use the no logging facility command.

**Parameters**

- **facility-type**
  - (OPTIONAL) Enter one of the following parameters:
    - auth (authorization system)
    - cron (Cron/at facility)
    - deamon (system deamons)
    - kern (kernel)
    - local0 (local use)
    - local1 (local use)
    - local2 (local use)
    - local3 (local use)
The default is **local7**.

### Defaults

**local7**

### 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*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series legacy command</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

- `logging` — enables logging to a Syslog server
- `logging on` — enables logging.
logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

Syntax

logging history level

To return to the default values, use the no logging history command.

Parameters

- **level**
  - Indicate a value from 0 to 7 or enter one of the following equivalent words: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 4 or warnings.

Defaults

warnings or 4

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>E-Series legacy command</td>
<td></td>
</tr>
</tbody>
</table>

Usage Information

When you configure the snmp-server trap-source command, the system messages logged to the history table are also sent to the SNMP network management station.

Related Commands

- **show logging** — displays information logged to the history buffer.

logging history size

Specify the number of messages stored in the Dell Networking logging history table.

Syntax

logging history size size

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.
To return to the default values, use the no logging history size command.

### Parameters

**size**  
Indicate a value as the number of messages to be stored. The range is from 0 to 500. The default is **1 message**.

### Defaults

**1 message**

### Command Modes

**CONFIGURATION**

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

**E-Series legacy command**

### Usage Information

When the number of messages reach the limit you set with the logging history size command, older messages are deleted as newer ones are added to the table.

### Related Commands

- `show logging` — displays information logged to the history buffer.

---

**logging monitor**

Specify which messages are logged to Telnet applications.

**Syntax**

`logging monitor [level]`

To disable logging to terminal connections, use the no logging monitor command.

**Parameters**

- **level**  
  Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is **7 or debugging**.

**Defaults**

**7 or debugging**
**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

**Related Commands**

- `default logging monitor` — returns the logging monitor parameters to the default setting.

---

**logging on**

Specify that debug or error messages are asynchronously logged to multiple destinations, such as the logging buffer, Syslog server, or terminal lines.

**Syntax**

```
logging on
```

To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

**Defaults**

Enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
Version | Description
--- | ---
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.2(1.0) | Introduced on the Z9500.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.

E-Series legacy command

Usage Information
When you use the no logging on command, messages are logged only to the console.

Related Commands
- logging — enable logging to the Syslog server.
- logging buffered — set the logging buffered parameters.
- logging console — set the logging console parameters.
- logging monitor — set the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

Syntax
logging source-interface interface

To disable this command and return to the default setting, use the no logging source-interface command.

Parameters
- **interface**
  Enter the following keywords and slot/port or number information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a Loopback interface, enter the keyword loopback then a number from 0 to 16383.
  - For the Management interface, enter the keyword ManagementEthernet then the slot/port information.
  - For a port-channel interface, enter the keywords port-channel then the port-channel ID.
  - For a Null interface, enter the keyword null then the Null interface number.
  - For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

Defaults
Not configured.

Command Modes
- CONFIGURATION
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking
OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.

Related Commands

- `logging` — enables logging to the Syslog server.

logging synchronous

Synchronize unsolicited messages and Dell Networking OS output.

Syntax

```
logging synchronous [level level | all] [limit number-of-buffers]
To disable message synchronization, use the no logging synchronous [level level | all] [limit number-of-buffers] command.
```

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enter the keyword all to ensure that all levels are printed asynchronously.</td>
</tr>
<tr>
<td>level level</td>
<td>Enter the keyword level then a number as the severity level. A high number indicates a low severity level and vice versa. The range is from 0 to 7. The default is 2.</td>
</tr>
<tr>
<td>all</td>
<td>Enter the keyword all to turn off all.</td>
</tr>
<tr>
<td>limit number-of-buffers</td>
<td>Enter the keyword limit then the number of buffers to be queued for the terminal after which new messages are dropped. The range is from 20 to 300. The default is 20.</td>
</tr>
</tbody>
</table>
Defaults

Disabled. If enabled without the level or number-of-buffers options specified, level = 2 and number-of-buffers = 20 are the defaults.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

When you enable logging synchronous, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands

- **logging on** — enables logging.

logging trap

Specify which messages are logged to the Syslog server based the message severity.

**Syntax**

`logging trap [level]`

To return to the default values, use the `default logging trap` command.

To disable logging, use the `no logging trap` command.

**Parameters**

- **level**
  
  Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 6 or informational.
Defaults

6 or informational

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series, S55.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Usage Information

To block a type of message parameter, set the logging trap level to a lower number. For example, to block severity messages at level 6, set the level to 5.

Related Commands

- `logging` — enables the logging to another device.
- `logging on` — enables logging.

logging version

Displays syslog messages in a RFC 3164 or RFC 5424 format.

Syntax

logging version {0|1}

Defaults

0

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
show logging auditlog

Displays an audit log.

Syntax

show logging auditlog
Defaults
None
Command Modes
EXEC
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL.</td>
</tr>
</tbody>
</table>

Example
Dell(conf)# show logging auditlog

Related Commands
• clear logging auditlog — clear the audit log.

show logging driverlog stack-unit
Display the driver log for the specified hardware component.

Syntax
show logging driverlog stack-unit stack-unit-number

Parameters
stack-unit stack-unit-number Enter the keywords stack-unit followed by the stack member ID of the switch for which you want to display the driver log.

defaults
none
Command Modes
• EXEC
• EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
9.2(0.0) | Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.

Example

```
Dell#show logging driverlog stack-unit 1
0:Task(tUsrRoot): [ 491677]PSU FanCtrl Drv ERR: ssnDrvPoePseEpromWriteEnable : 66 - Psu 1 is Not Present Cannot enable
1:Task(tUsrRoot): [ 338]PSU FanCtrl Drv ERR: ssnDrvPseFanCtrlInit : 118 - Cannot enable psu -127228353
2:Task(tUsrRoot): [ 6876]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Main block failed checksum calculated checksum 0x1d actual chksum 0x0
3:Task(tUsrRoot): [ 61]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Main block failed errcode 6
4:Task(tUsrRoot): [ 89]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Redundant block failed checksum calculated checksum 0xc9a6 actual chksum 0x0
5:Task(tUsrRoot): [ 57]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Redundant block failed errcode 6
6:Task(tUsrRoot): [ 51]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom, failed to get any good block
7:Task(tUsrRoot): [ 75]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Main block failed checksum calculated checksum 0x1d actual chksum 0x0
8:Task(tUsrRoot): [ 55]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Main block failed errcode 6
9:Task(tUsrRoot): [ 62]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Redundant block failed checksum calculated checksum 0xc9a6 actual chksum 0x0
10:Task(tUsrRoot): [ 55]EEPROM LIB ERR: f10EepromBlkRead@psu0eeeprom: Redundant block failed errcode 6
```  

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

**terminal monitor**

Configure the Dell Networking OS to display messages on the monitor/terminal.

**Syntax**

```
terminal monitor
```

To return to default settings, use the `terminal no monitor` command.

**defaults**

Disabled.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>

E-Series legacy command

Related Commands

- `logging monitor` — set the logging parameters on the monitor/terminal.
This section lists the traps sent by the Dell Networking OS. Each trap is listed by the fields `Message ID`, `Trap Type`, and `Trap Option`.

### Table 4. SNMP Trap List

<table>
<thead>
<tr>
<th>Message ID</th>
<th>Trap Type</th>
<th>Trap Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>COLD_START</td>
<td>SNMP</td>
<td>COLDSTART</td>
</tr>
<tr>
<td>%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARM_START</td>
<td>SNMP</td>
<td>WARMSTART</td>
</tr>
<tr>
<td>COPY_CONFIG_COMPLETE</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>SNMP Copy Config Command Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINK_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
</tr>
<tr>
<td>%IFA-1-PORT_LINKDN: changed interface state to down:%d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINK_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
</tr>
<tr>
<td>%IFA-1-PORT_LINKUP: changed interface state to up:%d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUTHENTICATION_FAIL</td>
<td>SNMP</td>
<td>AUTH</td>
</tr>
<tr>
<td>%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EGP_NEIGHBOR_LOSS</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>OSTATE_DOWN</td>
<td>SNMP</td>
<td>LINKDOWN</td>
</tr>
<tr>
<td>%IFM-1-OSTATE_DN: changed interface state to down:%s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSTATE_UP</td>
<td>SNMP</td>
<td>LINKUP</td>
</tr>
<tr>
<td>%IFM-1-OSTATE_UP: changed interface state to up:%s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>RMON_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM0-P:CP %SNMP-4- RMON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>falling threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_HC_RISING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM0-P:CP %SNMP-4- RMON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>high-capacity rising threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON_HC_FALLING_THRESHOLD</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%RPM0-P:CP %SNMP-4- RMON</td>
<td></td>
<td></td>
</tr>
<tr>
<td>high-capacity falling threshold alarm from SNMP OID &lt;oid&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BER_ERR</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%IFMGR-5-BER_ERR: High Ber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>detected on interface : %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BER_ERR_CLR</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%IFMGR-5-BER_ERR_CLR: High Ber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cleared on interface : %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAST_RETRAIN</td>
<td>SNMP</td>
<td>NONE</td>
</tr>
<tr>
<td>%IFMGR-5-FAST_RETRAIN: Retrain event detected on interface : %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESV</td>
<td>NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_CARD_PROBLEM</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_ALARM_CUTOFF</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_SFM_UP</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>CHM_RPM_UP</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%RAM-6-RPM_STATE: RPM1 is in Active State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-6-RPM_STATE: RPM0 is in Standby State</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_RPM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-2-RPM_DOWN: RPM 0 down - hard reset</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-RPM_DOWN: RPM 0 down - card removed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_RPM_PRIMARY</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>%RAM-5-COLD_FAILOVER: RPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-5-HOT_FAILOVER: RPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%RAM-5-FAST_FAILOVER: RPM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failover Completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_SFM_ADD</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TSM-5-SFM_DISCOVERY: Found SFM 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_SFM_REMOVE</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%TSM-5-SFM_REMOVE: Removed SFM 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_SFM_DOWN_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_SFM_DOWN</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-2-MINOR_SFM: Minor alarm: No working standby SFM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_SFM_DOWN_CLR</td>
<td>ENVMON</td>
<td>NONE</td>
</tr>
<tr>
<td>%CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_PWRSRC_DOWN</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_PWRSRC_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALARM_PS</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALARM_PS_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALARM_PS</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALARM_PS_CLR</td>
<td>ENVMON</td>
<td>SUPPLY</td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant</td>
<td>ENVMON TEMP</td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALRM_TEMP</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature</td>
<td>ENVMON TEMP</td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_ALRM_TEMP_CLR</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)</td>
<td>ENVMON TEMP</td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALRM_TEMP</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)</td>
<td>ENVMON TEMP</td>
<td></td>
</tr>
<tr>
<td>CHM_MAJ_ALRM_TEMP_CLR</td>
<td>TEMP</td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)</td>
<td>ENVMON TEMP</td>
<td></td>
</tr>
<tr>
<td>CHM_FANTRAY_BAD</td>
<td>FAN</td>
<td></td>
</tr>
<tr>
<td>For E1200: %CHMGR-2- FAN_TRAY_BAD: Major alarm: fan tray %d is missing or down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-ALL_FAN_BAD: Major alarm: all fans in fan tray %d are down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For E600 and E300: %CHMGR-2- FANTRAYBAD: Major alarm: fan tray is missing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_FANTRAY_BAD_CLR</td>
<td>FAN</td>
<td></td>
</tr>
<tr>
<td>For the E1200: %CHMGR-5- FAN_TRAY_OK: Major alarm cleared: fan tray %d present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For the E600 and E300: %CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHM_MIN_FANBAD</td>
<td>FAN</td>
<td></td>
</tr>
<tr>
<td>For the E1200: %CHMGR-2- FAN_BAD: Minor alarm: some fans in fan tray %d are down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>For the E600 and E300: %CHMGR-2-1FANBAD: Minor alarm: fan in fan tray is down</td>
<td>CHM_MIN_FANBAD_CLR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>For E1200: %CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good for E600 and E300: %CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good</td>
<td>TME_TASK_SUSPEND</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%TME-2-TASK_SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s</td>
<td>TME_TASK_TERM</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s</td>
<td>CHM_CPU_THRESHOLD</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)</td>
<td>CHM_CPU_THRESHOLD_CLR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)</td>
<td>CHM_MEM_THRESHOLD</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)</td>
<td>CHM_MEM_THRESHOLD_CLR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)</td>
<td>MACMGR_STN_MOVE</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d</td>
<td>PORT_TEMP_MAJOR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-1-PORT_TEMP_MAJOR: Major Alarm Interface %s shut due to high temperature</td>
<td>PORT_TEMP_MINOR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>%CHMGR-1-PORT_TEMP_MINOR: Minor Alarm Interface %s temperature exceeds threshold</td>
<td>PORT_TEMP_MAJOR_CLR</td>
<td>ENVMON</td>
</tr>
<tr>
<td>Message ID</td>
<td>Trap Type</td>
<td>Trap Option</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>%CHMGR-1-PORT_TEMP_MAJOR_CLR:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Alarm cleared for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface %s port temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>is lower than threshold</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VRRP_BADAUTH</th>
<th>PROTO</th>
<th>NONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>%RPM1-P:RP2 %VRRP-3-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VRRP BAD_AUTH: vrid-1 on Gi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/12 rcvd pkt with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication type mismatch.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| %RPM1-P:RP2 %VRRP-3-              |               |             |
| VRRP_BADAUTH: vrid-1 on Gi        |               |             |
| 11/12 rcvd pkt with               |               |             |
| authentication failure            |               |             |

<table>
<thead>
<tr>
<th>VRRP_GO_MASTER</th>
<th>PROTO</th>
<th>NONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>%VRRP-6-VRRP_MASTER: vrid-%d on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>%s entering MASTER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VRRP_PROTOCOL_ERROR</th>
<th>PROTO</th>
<th>NONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP_PROTOERR: VRRP protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>error on %S</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BGP4_ESTABLISHED</th>
<th>PROTO</th>
<th>NONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>%TRAP-5-PEER_ESTABLISHED:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neighbor %a, state %s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BGP4_BACKW_XSITION</th>
<th>PROTO</th>
<th>NONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>%TRAP-5-BACKWARD_STATE_TRANS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neighbor %a, state %s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
All commands in this chapter are specific to the Dell Networking OS.
You can use the commands to pre-configure a switch, so that the configuration settings are invoked when the switch is attached to other
S-Series units.

For information about using the S-Series stacking feature, see the Stacking S-Series Switches section in the Dell Networking OS Configuration Guide.

⚠️ **CAUTION**: You cannot enable stacking simultaneously with virtual link trunking (VLT). If you enable both at the same time,
unexpected behavior occurs.

The Dell Networking OS commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz
enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

Topics:
- redundancy disable-auto-reboot
- redundancy force-failover stack-unit
- redundancy protocol
- reset stack-unit
- show redundancy
- show system stack-ports
- stack-unit priority
- stack-unit provision
- stack-unit stack-group
- upgrade system stack-unit

redundancy disable-auto-reboot

Prevent the S-Series stack management unit, stack member unit, and standby unit from rebooting if they fail.

**Syntax**

```
redundancy disable-auto-reboot [stack-unit | members | stack-unit-number]
```

To return to the default, use the `no redundancy disable-auto-reboot stack-unit` command.

**Parameters**

- `stack-unit` Enter the stack-unit number. The range is from 1 to 6.
- `members` Enter the keyword members for all stack-units.

**Defaults**

Disabled (the failed switch is automatically rebooted).

**Command Mode**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
### show redundancy

Enabling this command keeps the failed switch in the Failed state. The switch does not reboot until it is manually rebooted. When enabled, it is not displayed in the running-config. When disabled, it is displayed in the running-config.

**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
```

**Parameters**

- `stack-unit` Enter the stack unit. The range is from 1 to 6.

**Defaults**

Not enabled.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

- **9.10(0.0)** Introduced on the S6100-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.
- **8.3.19.0** Introduced on the S4820T.
- **8.3.7.0** Introduced on the S4810.
- **8.3.11.1** Introduced on the Z9000.
- **8.3.1.0** Added the `members` option.

## redundancy protocol

Enable hitless failover for a protocol.

**Syntax**

```
redundancy protocol
```

**Usage Information**

Enable hitless failover for a protocol.
Protocols

lacp
Enter the LACP protocol

xstp
Enter one of the following protocols: STP, RSTP, MSTP, PVST.

Defaults
Not enabled.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the members option.</td>
</tr>
</tbody>
</table>

reset stack-unit

Reset any designated stack member except the management unit (master unit).

Syntax
reset stack-unit stack-unit-number hard

Parameters
stack-unit Enter the stack-unit number. The range is from 1 to 6.

hard Reset the stack unit if the unit is in a problem state.

Defaults
none

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Added the hard reset option.</td>
</tr>
</tbody>
</table>
Usage Information

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.

Starting with Dell Networking OS version 7.8.1.0, 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#reset stack-unit 4
Dell#00:15:00: %STKUNIT1-M:CP %CHMGR-5-STACKUNIT_RESET: stack-unit 4 being reset
00:15:01: %STKUNIT1-M:CP %CHMGR-2-STACKUNIT_DOWN: stack-unit 4 down - reset
00:15:01: %STKUNIT1-M:CP %IFMGR-1-DEL_PORT: Removed port: Gi 4/1-4/48, Te 4/51-4/52,
00:15:01: %STKUNIT2-S:CP %IFMGR-1-DEL_PORT: Removed port: Gi 4/1-4/48, Te 4/51-4/52,
Dell#00:15:08: %S3048-ON:1 %IFAGT-5-STACK_PORT_LINK_DOWN: Changed stack port state to down: 1/49
00:15:08: %STKUNIT1-M:CP %CHMGR-2-STACKUNIT_DOWN: stack-unit 4 down - card removed
Dell#

Related Commands

- reload — reboots Dell Networking OS.

show redundancy

Display the current redundancy configuration (status of automatic reboot configuration on stack management unit).

Syntax

show redundancy

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.8(2.0) Introduced on the S3100 series.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.7.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.

Usage Information

To modify your results, use the show redundancy [pipe] command, as follows:

- except — show only text that doesn not match a pattern.
- find — search for the first occurrence of a pattern.
- grep — show only text that matches a pattern.
- no-more — do not paginate the output.
- save — save the output to a file.
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:            1-0(0-3563)
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:           Disabled
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#

show system stack-ports

Display information about the stacking ports on all switches in the stack.

Syntax

show system stack-ports [status | topology]

Parameters

status          (OPTIONAL) Enter the keyword status to display the command output without the Connection field.

topology       (OPTIONAL) Enter the keyword topology to limit the table to just the Interface and Connection fields.

Defaults

none

Command Modes

  • EXEC
  • EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version | Description
---------|-------------
9.8(2.0) | Introduced on the S3100 series.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.7.0 | Introduced on the S4810.
8.3.11.1 | Introduced on the Z9000.

**Usage Information**
The following describes the show system stack-ports command shown in the following example.

**Field** | **Description**
--------|-------------
Topology | Lists the topology of stack ports connected: Ring, Daisy chain, or Standalone.
Interface | The unit/port ID of the connected stack port on this unit.
Link Speed | Link Speed of the stack port (10 or 40) in Gb/s.
Admin Status | The only currently listed status is Up.
Connection | 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 (Gb/s) Status Status
--------------------------------------------
1/49      2/49          12      up    up
1/50                      12      up    down
1/51      3/49          24      up    up
2/49      1/49          12      up    up
2/50      3/51          12      up    up
3/49      1/51          24      up    up
3/51      2/50          12      up    up
3/52                      12      up    down
Dell#

**Example (Status)**
Dell# show system stack-ports status
Topology: Daisy chain
Interface  Link Speed Admin Link (Gb/s) Status Status
--------------------------------------------
1/25       10            up        up
1/26       10            up        down
1/27       10            up        down
1/28       10            up        down
3/25       10            up        up
3/26       10            up        down
3/27       10            up        down
3/28       10            up        down
Dell# show system stack-ports status
Topology: Daisy chain
Interface  Link Speed Admin Link (Gb/s) Status Status
--------------------------------------------
1/25/1     10            up        up
1/26/1     10            up        down
1/27/1     10            up        down
1/28/1     10            up        down
3/25/1     10            up        up
3/26/1     10            up        down
Example (Topology)

Dell#show system stack-ports topology
Topology: Daisy chain
Interface   Connection
---------------------
1/25       3/25
1/26
1/27
1/28
3/25       1/25
3/26
3/27
3/28

Related Commands
• reset stack-unit — resets the designated stack member.
• 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 system (S-Series and Z-Series) — 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 priority-value

Parameters
stack-number Enter the stack member unit identifier.
priority-value This preference parameter allows you to specify the management priority of one backup switch over another, with 1 as the lowest priority and 14 being 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
1

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.
9.8(0.0P6) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.7.0 Introduced on the S4810.
8.3.11.1 Introduced on the Z9000.

Related Commands
• reload — reboots Dell Networking OS.
**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 [stack-number] provision {model-identifier}
```

**Parameters**

- `stack-number` Enter a stack member identifier of the switch that you want to add to the stack.
- `model-identifier` Enter the model identifier of the switch to be added as a stack member. This identifier is also referred to as the provision type.

**Defaults**

When this value is not set, a switch joining the stack is given the next available sequential stack member identifier.

**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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `reload` — reboot the Dell Networking OS.
- `show system (S-Series and Z-Series)` — display the status of all stack members or a specific member.

**stack-unit stack-group**

Configure the stacking unit and stacking group by specifying an ID when adding units to a stack to ensure the unit is assigned to the correct group.

**Syntax**

```
stack-unit unit-id stack-group stack-group-id
```

To remove the current stack group configuration, use the `no stack-unit unit-id stack-group stack-id` command.

**Parameters**

- `unit-id` Enter the stack unit ID.
- `stack-group-id` Enter the stack group ID.

**Defaults**

none

**Command Modes**

CONFIGURATION
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.1</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Reset command mode from EXEC to CONFIGURATION.</td>
</tr>
</tbody>
</table>

Usage Information
The following message displays to confirm the command.

Setting ports Fo 1/60 as stack group will make their interface configs obsolete after a reload. [confirm yes/no]: If "y" is entered, all non-default configurations on any member ports of the current stack group will be removed when the unit is rebooted.

NOTE: Any scripts used to streamline the stacking configuration process must be updated to reflect the Command Mode change from EXEC Privilege to CONFIGURATION to allow the scripts to work correctly.

upgrade system stack-unit

Copy the boot image or Dell Networking OS from the management unit to one or more stack members.

Syntax
upgrade {boot | system} stack-unit {all | stack-unit-number | A | B}

Parameters
- **boot**: Enter the keyword boot to copy the boot image from the management unit to the designated stack members.
- **system**: Enter the keyword system to copy the Dell Networking OS image from the management unit to the designated stack members.
- **stack-unit**: Enter the stack-unit number. The range is from 1 to 6.
- **all**: Enter the keyword all to copy the designated image to all stack members.
- **A**: Enter the keyword A to upgrade all stacked units in System A (only).
- **B**: Enter the keyword B to upgrade all stacked units in System B (only).

Defaults
- none

Command Modes
- EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(2.0)</td>
<td>Introduced on the S3100 series.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

To reboot using the new image, use the `upgrade boot system stack-unit` command.

Related Commands

- `reload` — reboots Dell Networking OS.
- `reset stack-unit` — resets the designated stack member.
- `show system (S-Series and Z-Series)` — displays the status of all stack members or a specific member.
- `show version` — displays the current Dell Networking OS version information on the system.
The Dell Networking OS storm control feature allows you to limit or suppress traffic during a traffic storm (Broadcast/Unknown Unicast Rate Limiting or Multicast on the C-Series and S-Series).

Storm control is supported on Dell Networking OS.

Important Points to Remember

- Interface commands can only be applied on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- You can apply the CONFIGURATION-level storm control commands at ingress or egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. It is not based on the speed setting for the line card.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).
- When you enable broadcast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic goes to queue 1 instead of queue 0.
- Similarly, if you enable unicast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic goes to queue 2 instead of queue 0.

**NOTE:** Bi-directional traffic (unknown unicast and broadcast) along with egress storm control causes the configured traffic rates split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port pipes or the same/different line cards.

**NOTE:** The policy discard drop counters are common across storm-control drops, ACL drops and QoS drops. If your configuration includes ACL and QoS, those drops are also computed and displayed in the policy discard drops counter field along with storm-control drops. The packets dropped by the storm control feature can be monitored by viewing the value of the Policy Discard Drops field of the output of the show hardware stack-unit stack-unit-number drops command.

Topics:

- show storm-control broadcast
- show storm-control multicast
- show storm-control unknown-unicast
- storm-control broadcast (Configuration)
- storm-control broadcast (Interface)
- storm-control multicast (Configuration)
- storm-control multicast (Interface)
- storm-control PFC/LLFC
- storm-control unknown-unicast (Configuration)
- storm-control unknown-unicast (Interface)
show storm-control broadcast

Display the storm control broadcast configuration.

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 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

show storm-control multicast

Display the storm control multicast configuration.

Syntax

```
show storm-control multicast [interface]
```

show storm-control multicast
Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration:

- For a 1-Gigabit Ethernet interface, enter the keyword GigabitEthernet then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
- For a port channel interface, enter the keywords port-channel then a number.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Example

Dell# show storm-control multicast gigabitethernet 1/1
Multicast storm control configuration
Interface     Direction   Packets/Second
-------------- ------------- --------------------------
Gi 1/1         Ingress      5

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

Syntax

show storm-control unknown-unicast [interface]
Parameters

- **interface** (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a port channel interface, enter the keywords `port-channel` then a number.

Defaults

- **None**

Command Modes

- **EXEC**
- **EXEC Privilege**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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.
**storm-control broadcast** [percentage decimal_value in | out] [wred-profile name] [packets_per_second in]

To disable broadcast rate-limiting, use the **storm-control broadcast** [percentage decimal_value in | out] [wred-profile name] [packets_per_second in] command.

**Parameters**
- **percentage decimal_value in | out**
  Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. The decimal range is from .1 to .9.

- **wred-profile name**
  Enter the keyword wred-profile followed by the profile name to designate a wred-profile.

- **packets_per_second in**
  Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

**Defaults**
- none

**Command Modes**
- CONFIGURATION (conf)

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the S6100-ON.
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 M I/O Aggregator. This command is supported in Programmable-MUX (PMUX) mode only.
8.3.19.0 | Introduced on the S4820T.
8.3.11.1 | Introduced on the Z9000.
8.3.7.0 | Introduced on the S4810.
7.6.1.0 | Introduced on the S-Series.
7.5.1.0 | Introduced on the C-Series.
7.4.1.0 | E-Series Only: Added the percentage decimal_value option.
6.5.1.0 | Introduced on the E-Series.

**Usage Information**
Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

**storm-control broadcast (Interface)**

Configure the percentage of broadcast traffic allowed on an interface (ingress only).

**Syntax**

```
storm-control broadcast [packets_per_second in]
```

1466 | Storm Control
To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second in]` command.

**Parameters**

- `packets_per_second in` Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

**Defaults**

`none`

**Command Modes**

`INTERFACE (conf-if-interface-slot/port)`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series Only: Added the <code>percentage decimal value</code> option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**storm-control multicast (Configuration)**

Configure the packets per second (pps) of multicast traffic allowed into the C-Series and S-Series networks only.

**Syntax**

```plaintext
storm-control multicast packets_per_second in
```

To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.

**Parameters**

- `packets_per_second in` Enter the packets per second of multicast traffic allowed into the network. The range is from 0 to 33554368.

**Defaults**

`none`

**Command Modes**

`CONFIGURATION (conf)`
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-MUX (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-series and S-Series.</td>
</tr>
</tbody>
</table>

Broadcast traffic (all 0xFs) should be counted against the broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that some multicast control traffic may get dropped when storm control thresholds are exceeded.

**storm-control multicast (Interface)**

Configure the percentage of multicast traffic allowed on a C-Series or S-Series interface (ingress only) network only.

**Syntax**

```
storm-control multicast packets_per_second in
```

To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

**Parameters**

- `packets_per_second in` Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

**Defaults**

none

**Command Modes**

INTERFACE (conf-if-interface-slot/port)

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
storm-control PFC/LLFC

Shut down the port if it receives the PFC/LLFC frames more than the configured rate.

Syntax

```
storm-control pfc-llfc \[pps\]in shutdown
```

Parameters

- `pfc-llfc in` Enter the keyword `pfc-llfc` to get the flow control traffic. The range is from 0 to 33554368 packets per second.
- `shutdown` Enter the keyword `shutdown` 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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010, S4810, S4820T, S5000, S6000, Z9500, S3048-ON, S4048-ON, and S6000-ON.</td>
</tr>
</tbody>
</table>

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 in or out of the network.

Syntax

```
storm-control unknown-unicast \[packets_per_second in\]
```

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast \[packets_per_second in\]` command.

Parameters

- `packets_per_second in` Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

CONFIGURATION
### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series Only: Added the percentage decimal value option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

### storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (ingress only).

**Syntax**

```
storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]] [packets_per_second in]
```

To disable unknown-unicast storm control on the interface, use the no storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]] [packets_per_second in] command.

**Parameters**

- **percentage decimal_value [in | out]**
  
  E-Series Only: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%.

  The percentage is from 0 to 100:
  - 0% blocks all related traffic.
  - 100% allows all traffic into the interface.

  The decimal range is from 0.1 to 0.9.

- **wred-profile name**
  
  E-Series Only: (Optionally) Enter the keywords wred-profile followed by the profile name to designate a wred-profile.

- **packets_per_second in**
  
  C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554431.
Defaults: none

Command Modes: INTERFACE (conf-if-interface-slot/port)

Command History: This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.4.1.0</td>
<td>E-Series Only: Added the percentage decimal value option.</td>
</tr>
<tr>
<td>6.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Spanning Tree Protocol (STP)

The commands in this section configure and monitor the IEEE 802.1d spanning tree protocol (STP) and are supported on the Dell Networking switch/routing platform.

Topics:
- bridge-priority
- bpdu-destination-mac-address
- debug spanning-tree
- description
- disable
- forward-delay
- hello-time
- max-age
- protocol spanning-tree
- show config
- show spanning-tree 0
- spanning-tree

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

Syntax

```
bridge-priority {priority-value | primary | secondary}
```

To return to the default value, use the `no bridge-priority` command.

Parameters

- **priority-value**: Enter a number as the bridge priority value. The range is from 0 to 65535. The default is 32768.
- **primary**: Enter the keyword primary to designate the bridge as the root bridge.
- **secondary**: Enter the keyword secondary to designate the bridge as a secondary root bridge.

Defaults

priority-value = 32768

Command Modes

SPANNING TREE (The prompt is “config-stp.”)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.10(0.0) | Introduced on the S6100–ON.
9.8(10) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
bpdu-destination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Syntax
bpdu-destination-mac-address [stp | gvrp] provider-bridge-group

Parameters
- **xstp**: Force STP, RSTP, and MSTP to use the Provider Bridge Group address as the destination MAC address in its BPDUs.
- **gvrp**: Forces GVRP to use the Provider Bridge GVRP Address as the destination MAC address in its PDUs.

Defaults
The destination MAC address for BPDUs is the Bridge Group Address.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Spanning Tree Protocol (STP) | 1473
**debug spanning-tree**

Enable debugging of the spanning tree protocol and view information on the protocol.

**Syntax**
```
debug spanning-tree {stp-id | all | bpdu | config | events | exceptions | general | root} | protocol
```
To disable debugging, use the no debug spanning-tree command.

**Parameters**
- **stp-id**
  - Enter zero (0). The switch supports one spanning tree group with a group ID of 0.
- **protocol**
  - Enter the keyword for the type of STP to debug, either mstp, pvst, or rstp.
- **all**
  - (OPTIONAL) Enter the keyword all to debug all spanning tree operations.
- **bpdu**
  - (OPTIONAL) Enter the keyword bpdu to debug bridge protocol data units.
- **config**
  - (OPTIONAL) Enter the keyword config to debug configuration information.
- **events**
  - (OPTIONAL) Enter the keyword events to debug STP events.
- **general**
  - (OPTIONAL) Enter the keyword general to debug general STP operations.
- **root**
  - (OPTIONAL) Enter the keyword root to debug STP root transactions.

**Command Modes**
- EXEC Privilege

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
When you enable debug spanning-tree bpdu for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

**Related Commands**
- **protocol spanning-tree** — enters SPANNING TREE mode on the switch.
**description**

Enter a description of the spanning tree.

**Syntax**

description {description}  
To remove the description from the spanning tree, use the no description {description} command.

**Parameters**

- **description**  
Enter a description to identify the spanning tree (80 characters maximum).

**Defaults**

none

**Command Modes**

SPANNING TREE (The prompt is "config-stp").

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the S6100–ON.
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.
7.7.1.0 | Introduced

**Related Commands**

- protocol spanning-tree — enter SPANNING TREE mode on the switch.

**disable**

Disable the spanning tree protocol globally on the switch.

**Syntax**

disable  
To enable Spanning Tree Protocol, use the no disable command.

**Defaults**

Enabled (that is, the spanning tree protocol is disabled.)

**Command Modes**

SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Related Commands

- **protocol spanning-tree** — enter SPANNING TREE mode on the switch.

### forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

**Syntax**

```plaintext
forward-delay seconds
```

To return to the default setting, use the `no forward-delay` command.

**Parameters**

- `seconds` Enter the number of seconds the Dell Networking OS waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is 15 seconds.

**Defaults**

15 seconds

**Command Modes**

- **SPANNING TREE**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

#### Version

- 9.10(0.0) Introduced on the S6100–ON.
- 9.8(1.0) Introduced on the Z9100–ON.
- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Introduced on the S6000-ON.
- 9.2(1.0) Introduced on the Z9500.
- 9.0.2.0 Introduced on the S6000.
- 8.3.11.1 Introduced on the Z9000.
- 8.3.7.0 Introduced on the S4810.
- 7.7.1.0 Introduced on the S-Series.
- 7.5.1.0 Introduced on the C-Series.
- 6.2.1.1 Introduced on the E-Series.

### forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

**Syntax**

```plaintext
forward-delay seconds
```

To return to the default setting, use the `no forward-delay` command.

**Parameters**

- `seconds` Enter the number of seconds the Dell Networking OS waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is 15 seconds.

**Defaults**

15 seconds

**Command Modes**

- **SPANNING TREE**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

#### Version

- 9.10(0.0) Introduced on the S6100–ON.
- 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.
### hello-time

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

**Syntax**

```markdown
hello-time seconds
```

To return to the default value, use the `no hello-time` command.

**Parameters**

- **seconds**: Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

**Defaults**

- **2 seconds**

**Command Modes**

- SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7(1.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5(1.0)</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2(1.1)</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Related Commands

- `forward-delay` — changes the wait time before STP transitions to the Forwarding state.
- `max-age` — changes the wait time before STP refreshes protocol configuration information.

**max-age**

To maintain configuration information before refreshing that information, set the time interval for the spanning tree bridge.

**Syntax**

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

**Parameters**

- `seconds` Enter a number of seconds the Dell Networking OS waits before refreshing configuration information. The range is from 6 to 40. The default is 20 seconds.

**Defaults**

- 20 seconds

**Command Modes**

- SPANNING TREE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `forward-delay` — changes the wait time before STP transitions to the Forwarding state.
- `hello-time` — changes the time interval between BPDUs.

**protocol spanning-tree**

To enable and configure the spanning tree group, enter SPANNING TREE mode.

**Syntax**

```
protocol spanning-tree stp-id
```

**Related Commands**

- `forward-delay` — changes the wait time before STP transitions to the Forwarding state.
- `hello-time` — changes the time interval between BPDUs.
To disable the Spanning Tree group, use the `no protocol spanning-tree stp-id` command.

**Parameters**

- **stp-id**
  - Enter zero (0). Dell Networking OS supports one spanning tree group, group 0.

**Defaults**

- Not configured.

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**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**

```plaintext
show spanning-tree 0 [active | brief | guard | interface interface | root | summary]
```

**Parameters**

- **0**
  - Enter 0 (zero) to display information about that specific spanning tree group.
- **active**
  - (OPTIONAL) Enter the keyword `active` to display only active interfaces in spanning tree group 0.
- **brief**
  - (OPTIONAL) Enter the keyword `brief` to display a synopsis of the spanning tree group configuration information.
- **guard**
  - (OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an STP interface and the current port state.
- **interface interface**
  - (OPTIONAL) Enter the keyword `interface` and the type slot/port of the interface you want displayed. Type slot/port options are the following:
    - For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.
    - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
    - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- **root**
  - (OPTIONAL) Enter the keyword `root` to display configuration information on the spanning tree group root.
summary (OPTIONAL) Enter the keyword summary to only the number of ports in the spanning tree group and their state.

Command Modes EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards on the E-Series.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Added support for the optional guard keyword on the C-Series, S-Series, and E-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
Enable spanning tree group 0 prior to using this command.

The following describes the show spanning-tree 0 command shown in the example.

Field          Description
"Bridge Identifier..." Lists the bridge priority and the MAC address for this STP bridge.
"Configured hello..." Displays the settings for hello time, max age, and forward delay.
"We are..." States whether this bridge is the root bridge for the STG.
"Current root..." Lists the bridge priority and MAC address for the root bridge.
"Topology flag..." States whether the topology flag and the detected flag were set.
"Number of..." Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
"Timers" Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
"Times" List the number of seconds since the last:
  • hello time
  • topology change
  • notification
Field Description

- aging

"Port 1..." Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).

"Port path..." Displays the path cost, priority, and identifier for the interface.

"Designated root..." Displays the priority and MAC address of the root bridge of the STG that the interface belongs.

"Designated port..." Displays the designated port ID.

Example

Dell# show spann 0

Executing IEEE compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Current root has priority 32768 address 0001.e800.0a56
Topology change flag set, detected flag set
Number of topology changes 1 last change occurred 0:00:05 ago
from GigabitEthernet 1/3
Timers:hold 1, topology change 35
  hello 2, max age 20, forward_delay 15
Times:hello 1, topology change 1, notification 0, aging 2

Port 26 (GigabitEthernet 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
BPU: sent:18, received 0
The port is not in the portfast mode

Port 27 (GigabitEthernet 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
BPU: sent:18, received 0
The port is not in the portfast mode

Port 28 (GigabitEthernet 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
BPU: sent:31, received 0
The port is not in the portfast mode

Dell#

Example (Brief)

Dell# show span 0 brief

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768
  Address 0001.e800.0a56
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768,
  Address 0001.e800.0a56
Configured hello time 2, max age 20, forward delay 15
Interface Designated
Name | PortID | Prio | Cost | Sts | Cost | Bridge ID | PortID
--- | ------ | ---- | ---- | --- | ---- | --------- | ------
Gi 1/1 | 8.26 | 8   | 4   | FWD | 0    | 32768 0001.e800.0a56 | 8.26
Gi 1/2 | 8.27 | 8   | 4   | FWD | 0    | 32768 0001.e800.0a56 | 8.27
Gi 1/3 | 8.28 | 8   | 4   | FWD | 0    | 32768 0001.e800.0a56 | 8.28

Usage Information
The following describes the show spanning-tree 0 guard command shown in the example.

Field | Description
--- | ---
Interface Name | STP interface.
Instance | STP 0 instance.
Sts | Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type | Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)
Dell#show spanning-tree 0 guard
Interface
Name | Instance | Sts | Guard type
--- | --- | --- | ---
Gi 1/1 | 0 | INCON(Root) | Rootguard
Gi 1/2 | 0 | LIS | Loopguard
Gi 1/3 | 0 | EDS (Shut) | Bpduguard

spanning-tree
Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

Syntax
```
spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast [bpduguard [shutdown-on-violation]] | priority priority}
```

To disable Spanning Tree group on an interface, use the no spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast [bpduguard [shutdown-on-violation]] | priority priority} command.

Parameters
- **stp-id**
Enter the STP instance ID. The range is 0.
- **cost cost**
Enter the keyword cost then a number as the cost. The range is from 1 to 65535. The defaults are:
  - 1-Gigabit Ethernet interface = 4.
  - 10-Gigabit Ethernet interface = 2.
  - Port Channel interface with 100 Mb/s Ethernet = 18.
  - Port Channel interface with 1 Gigabit Ethernet = 3.
  - Port Channel interface with 10 Gigabit Ethernet = 1.
- **loopguard**
Enter the keyword loopguard to enable STP loop guard on a port or port-channel interface.
- **rootguard**
Enter the keyword rootguard to enable STP root guard on a port or port-channel interface.
portfast [bpdu guard] [shutdown-on-violation]

Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails.

Enter the optional keyword `bpdu guard` to disable the port when it receives a BPDU.

Enter the optional keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

priority priority

Enter keyword `priority` then a number as the priority. The range is from zero (0) to 15. The default is 8.

Defaults

cost = depends on the interface type; priority = 8

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.10.1</td>
<td>Introduced the <code>loopguard</code> and <code>rootguard</code> options on the S4810.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>Introduced the <code>loopguard</code> and <code>rootguard</code> options on the E-Series, C-Series, and S-Series.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced the <code>shutdown-on-violation</code> option.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If you enable `portfast bpdu guard` 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, BPDU's are still sent to the RPM CPU.

STP loop guard and root guard are supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST+).
Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.

STP root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: 

```
% Error: RootGuard is configured. Cannot configure LoopGuard.
```

Do not enable Portfast BPDU guard and loop guard at the same time on a port. Enabling both features may result in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

To display the type of STP guard (Portfast BPDU, root, or loop guard) enabled on a port, enter the `show spanning-tree` command.
SupportAssist

SupportAssist sends troubleshooting data securely to Dell. SupportAssist in this Dell Networking OS release does not support automated email notification at the time of hardware fault alert, automatic case creation, automatic part dispatch, or reports. SupportAssist requires Dell Networking OS 9.9(0.0) and SmartScripts 9.7 or later to be installed on the Dell Networking device. For more information on SmartScripts, see Dell Networking Open Automation guide.

NOTE: SupportAssist is enabled by default on the system. To disable SupportAssist, enter the `eula-consent support-assist reject` command in Global Configuration mode and save the configuration.

Topics:
- `eula-consent`
- `support-assist`
- `support-assist activate`
- `support-assist activity`
- SupportAssist Commands
- SupportAssist Activity Commands
- SupportAssist Company Commands
- SupportAssist Person Commands
- SupportAssist Server Commands
- `show eula-consent`
- `show running-config`
- `show support-assist status`

**eula-consent**

Accept or reject the end user license agreement (EULA).

**Syntax**

```
eula-consent {support-assist} {accept | reject}
```

**Parameters**

- **support-assist**
  - Enter the keywords `support-assist` to either accept or reject the EULA for the specified service.
- **accept**
  - Enter the keyword `accept` to accept the EULA for the specified service.
- **reject**
  - Enter the keyword `reject` to reject the EULA for the specified service.

**Defaults**

None

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
</tbody>
</table>
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

Dell(conf)# eula-consent support-assist accept
I accept the terms of the license agreement. You can reject the license agreement by configuring this command 'eula-consent support-assist reject'.

By installing SupportAssist, you allow Dell to save your contact information (e.g. name, phone number and/or email address) which would be used to provide technical support for your Dell products and services. Dell may use the information for providing recommendations to improve your IT infrastructure.

Dell SupportAssist also collects and stores machine diagnostic information, which may include but is not limited to configuration information, user supplied contact information, names of data volumes, IP addresses, access control lists, diagnostics & performance information, network configuration information, host/server configuration & performance information and related data ("Collected Data") and transmits this information to Dell. By downloading SupportAssist and agreeing to be bound by these terms and the Dell end user license agreement, available at: www.dell.com/aeula, you agree to allow Dell to provide remote monitoring services of your IT environment and you give Dell the right to collect the Collected Data in accordance with Dells Privacy Policy, available at: www.dell.com/privacypolicycountryspecific, in order to enable the performance of all of the various functions of SupportAssist during your entitlement to receive related repair services from Dell. You further agree to allow Dell to transmit and store the Collected Data from SupportAssist in accordance with these terms. You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dells affiliates, subcontractors or business partners. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Collected Data being transferred in connection with SupportAssist. If you are downloading SupportAssist on behalf of a company or other legal entity, you are further certifying to Dell that you have appropriate authority to provide this consent on behalf of that entity. If you do not consent to the collection, transmission and/or use of the Collected Data, you may not download, install or otherwise use SupportAssist.

Related Commands

- support-assist — moves to the SupportAssist Configuration mode.
support-assist

Move to the SupportAssist configuration mode.

Syntax

support-assist

To remove all the configuration of the SupportAssist service, use the no support-assist command.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

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

Enable the SupportAssist service.

Syntax

support-assist activate

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

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.

support-assist activity

Trigger an activity event immediately.

Syntax

support-assist activity {full-transfer} start now

1488  |  SupportAssist
Parameters

**full-transfer**

Enter the keywords `full-transfer` to specify transfer of configuration, inventory, logs, and other information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
contact-company

Configure the contact information for the company.

Syntax

```plaintext
contact-company name {company-name}[company-next-name] ... [company-next-name]
```

To remove the contact company information, use the `no contact-company` command.

Parameters

- **company-name**
  - Enter the name for the company. If there are multiple words in the name, use optional additional fields.

- **company-next-name**
  - (Optional) Enter the next components of the company name, up to 5 components are allowed.

Command Modes

SUPPORTASSIST

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

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

```plaintext
contact-person [first <first-name>] last <last-name>
```

To remove the contact person and all their details, use the `no contact-person [first <first-name>] last <last-name>` command.

Parameters

- **first-name**
  - (Optional) Enter the first name for the contact person. This is optional provided each contact person name is unique. To include a space, enter a space within double quotes.

- **last-name**
  - Enter the last name for the contact person. To include a space, enter a space within double quotes.

Command Modes

SUPPORTASSIST

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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 servers for the SupportAssist service.

**Syntax**

```
enable all
```

To return to the default setting, use the `no enable all` command.

**Parameters**

- `all` Enter the keyword `all` to enable all SupportAssist service activities.

**Defaults**

Enabled or All Enabled

**Command Modes**

SUPPORTASSIST

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
9.9(0.0) | Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**server**

Configure the name of the remote SupportAssist Server and move to SupportAssist Server mode.

**Syntax**

```
server {default | server-name}
```

To delete a server, use the `no server server-name` command.

**Parameters**

- `default` Enter the keyword `default` for the default server.
- `server-name` Enter the name of the remote SupportAssist Server. To include a space, enter a space within double quotes.

**Defaults**

Default server has URL stor.g3.ph.dell.com

**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.
SupportAssist Activity Commands

Dell Networking OS supports the following SupportAssist Activity mode commands.

action-manifest get

Copy an action-manifest file for an activity to the system.

Syntax

```
action-manifest get tftp | ftp | flash <file-specification> <local-file-name>
```

Parameters

- `file-specification` Enter the full file specification for the action-manifest file. For example:
  - tftp://hostip/filepath
  - ftp://userid:password@hostip/filepath
  - scp://userid:password@hostip/filepath

- `local-file-name` Enter the name of the local action-manifest file, up to 32 characters long. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

Command Modes

- SUPPORTASSIST ACTIVITY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version | Description
--- | ---
9.10(0.0) | Introduced on the C9010, 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.

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 the action-manifest to use for a specific activity.

Syntax

```
action-manifest install {default | <local-file-name>}
```

To revert to the default action-manifest file, use the `action-manifest install default` command.

Parameters

- **default**
  - Enter the keyword `default` to revert back to the default set of actions for an activity.

- **local-file-name**
  - Enter the name of the local action-manifest file. Allowable characters are: a to z, A to Z, 0 to 9, _, and space.

Defaults

Default

Command Modes

SUPPORTASSIST ACTIVITY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the C9010, 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 put` 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 for an activity.

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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.10(0.0): Introduced on the C9010, Z9100-ON, S6100-ON, and S3100 series.
- 9.9(0.0): Introduced on the S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, Z9500, MXL.

**Related Commands**

- `action-manifest get` — copy an action-manifest file for an activity to the system.
- `action-manifest install` — configure the action-manifest to use for a specific activity.
- `action-manifest remove` — remove the action-manifest file for an activity.

**enable**

Enable a specific SupportAssist activity.

**Syntax**

```
enable
```

**Default**

Enabled

**Command Modes**

- SUPPORTASSIST ACTIVITY

To disable a particular SupportAssist activity, use the `no enable` command.
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the C9010, 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**
- activity — move user to the SupportAssist Activity mode for that activity.

## SupportAssist Company Commands

Dell Networking OS supports the following SupportAssist Company mode commands.

### address

Configure the address information for the company.

**Syntax**

```
address [city company-city] [(province | region | state) name] [country company-country] [(postalcode | zipcode) company-code]
```

To remove a portion of the company address information, use the `no address [city | province | region | state | country | postalcode | zipcode]` command.

To remove the complete company contact information, use the `no address` command.

**Parameters**

- `city company-city` (OPTIONAL) Enter the keyword `city` then the city or town for the company site. To include a space, enter a space within double quotes.
- `province | region | state name` (OPTIONAL) Enter the keyword `province`, `region` or `state` then the name of province, region or state for the company site. To include a space, enter a space within double quotes.
- `country company-country` (OPTIONAL) Enter the keyword `country` then the country for the company site. To include a space, enter a space within double quotes.
- `postalcode | zipcode company-code` (OPTIONAL) Enter the keyword `postalcode` or `zipcode` then the postal code or zip code for the company site, as one string with no spaces.

**Command Modes**

SUPPORTASSIST COMPANY

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version** | **Description**
--- | ---
9.10(0.0) | Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0) | Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.
Usage Information

The optional parameters must be provided in the following order: city state country postalcode. If specified in a different order, the command returns an error as follows:

```
Dell(conf-supportassist-cmpy-test)# address city Minneapolis postalcode 55344 country USA state Minnesota | ^
% Error: Invalid input at "^" marker.
```

This command is optional for SupportAssist service configuration.

Example

```
Dell(conf-supportassist-cmpy-test)# address city Minneapolis state Minnesota country USA postalcode 55344
```

street-address

Configure the street address information for the company.

```
Syntax

street-address {address1} [address2]...[address8]
To remove the street address, use the no street-address command.

Parameters

address1 Enter the street address for the company.
address2..address8 (OPTIONAL) Enter the street address of the company site. Up to 8 fields are allowed.

Command Modes

SUPPORTASSIST COMPANY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.10(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.

Command Modes

SUPPORTASSIST COMPANY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.10(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.
```
### SupportAssist Person Commands

Dell Networking OS supports the following SupportAssist Person mode commands.

#### email-address

Configure the email addresses to reach the contact person.

**Syntax**

```plaintext
e-mail-address primary email-address [alternate email-address]
```

To remove an email address, use either the `no email-address primary` or `no email-address alternate` commands.

**Parameters**

- `primary email-address`
  - Enter the keyword `primary` then the primary email address for the person.

- `alternate email-address`
  - Enter the keyword `alternate` then the alternate email address for the person.

**Command Modes**

- SUPPORTASSIST PERSON

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.10(0.0)  Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
- 9.9(0.0)   Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

**Usage Information**

The email addresses must have the standard form of `<username>@<email system>` to be considered valid.

This command is optional for SupportAssist service configuration.

**Related Commands**

- `preferred-method` — configure the preferred method for contacting the person.

#### phone

Configure phone numbers to reach the contact person.

**Syntax**

```plaintext
phone primary phone [alternate phone]
```

**Usage Information**

This command is optional for SupportAssist service configuration.
To remove a phone number, use either the `no phone primary` or `no phone alternate` commands.

**Parameters**

- **primary phone**
  - Enter the keyword `primary` then the primary phone number for the person.

- **alternate phone**
  - Enter the keyword `alternate` then the alternate phone number for the person.

**Command Modes**

- SUPPORTASSIST PERSON

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

**Usage Information**

The phone numbers may contain country codes, area codes and extensions, if necessary. Allowable characters are 0 to 9, x, ( ), - and +.

This command is optional for SupportAssist service configuration.

**Related Commands**

- `preferred-method` — configure the preferred method for contacting the person.

---

**preferred-method**

Configure the preferred method for contacting the person.

**Syntax**

```
preferred-method {email | no-contact | phone}
```

**Parameters**

- **email**
  - Enter the keyword `email` to specify email as preferred method.

- **no-contact**
  - Enter the keywords `no-contact` to specify that there is no preferred method.

- **phone**
  - Enter the keyword `phone` to specify phone as preferred method.

**Defaults**

- `no-contact`

**Command Modes**

- SUPPORTASSIST PERSON

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `email-address` — configure email addresses to reach the contact person.
- `phone` — configure phone numbers to reach the contact person.
time-zone

Configure the time zone for contacting the person.

Syntax

time-zone zone +HH:MM[start-time HH:MM] [end-time HH:MM]
To remove the time zone, use the no time-zone [zone | start-time | end-time] command.

Parameters

zone +HH:MM Enter the keyword zone then a time difference from GMT expressed as HH:MM. This number may be preceded by either a + or – sign.

start-time HH:MM Enter the keywords start-time then a starting time expressed as HH:MM. Use the 24-hour clock format.

stop-time HH:MM Enter the keywords stop-time then a stopping time expressed as HH:MM. Use the 24-hour clock format.

Command Modes

SUPPORTASSIST PERSON

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0) Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information
This command is optional for SupportAssist service configuration.

SupportAssist Server Commands

Dell Networking OS supports the following SupportAssist Server mode commands.

proxy-ip-address

Configure a proxy for reaching the SupportAssist remote server.

Syntax

proxy-ip-address {ipv4-address | ipv6-address} port port-number [ username userid password [encryption-type] password ]
To remove the proxy, use the no proxy-ip-address command.

Parameters

ipv4-address Enter the IP address of the proxy server in a dotted decimal format (A.B.C.D).

ipv6-address Enter the IPv6 address of the proxy server in the x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

NOTE: To use the IPv6 address, the Open Automation package should also support IPv6 communications. For this purpose, SupportAssist requires Dell Networking Open Automation 9.10(0.0) package or later.
```
port port-number
username userid
password
encryption-type

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

Usage Information

- The passwords are stored encrypted in the running configuration.

**enable**

Enable communication with the SupportAssist server.

```
Syntax

```

```

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>
```

Related Commands

- server — configure the name of the remote SupportAssist server.
url

Configure the URL to reach the SupportAssist remote server.

Syntax

```
url uniform-resource-locator
```

To delete the URL for the server, use the `no url` command.

Parameters

```
uniform-resource-locator
```

Enter a text string for the URL using one of the following formats:

- `http://[username:password@]<hostip>:<portNum>/<filepath>`
- `https://[username:password@]<hostip>:<portNum>/<filepath>`

**NOTE:** The host IP for the server may be specified as an IPv4 address, an IPv6 address or as a DNS hostname. If using the DNS hostname, the DNS resolver will need to be configured and enabled.

Command Modes

SUPPORTASSIST SERVER

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.10(0.0) Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0) Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.
```

Usage Information

The URL should be formatted to follow the ISO format.

show eula-consent

Display the EULA for the feature.

Syntax

```
show eula-consent {support-assist | other feature}
```

Parameters

```
support-assist | other feature
```

Enter the keywords `support-assist` or the text corresponding to other feature.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

```
Version Description
9.10(0.0) Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0) Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.
```

Example

```
Dell# show eula-consent
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 in accordance with these terms. You agree that the provision of SupportAssist may involve international transfers of data from you to Dell and/or to Dells affiliates, subcontractors or business partners. When making such transfers, Dell shall ensure appropriate protection is in place to safeguard the Collected Data being transferred in connection with SupportAssist. If you are downloading SupportAssist on behalf of a company or other legal entity, you are further certifying to Dell that you have appropriate authority to provide this consent on behalf of that entity. If you do not consent to the collection, transmission and/or use of the Collected Data, you may not download, install or otherwise use SupportAssist.

Dell#

**show running-config**

Display the current configuration and changes from the default values.

**Syntax**

```
show running-config support-assist
```

**Parameters**

- `support-assist`: Enter the keyword support-assist to view the detailed configuration for the feature.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**show support-assist status**

Display information on SupportAssist feature status including any activities, status of communication, last time communication sent, and so on.

**Syntax**

```
show support-assist status
```

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell# show support-assist status
SupportAssist Service: Installed
EULA: Accepted
Server: default
  Enabled: Yes
  URL: https://stor.g3.ph.dell.com
Service status: Enabled
Server: chennai
  Enabled: Yes
  URL: http://10.16.148.19/

Activity      State   Last Start  Last Success
------------  ----------------------------
full-transfer Failure
Dell#
```

Dell# show support-assist status
SupportAssist Service: Installed
EULA: Accepted
Server: default
  Enabled: Yes
  URL: https://stor.g3.ph.dell.com
Service status: Enabled
Server: chennai
  Enabled: Yes
  URL: http://10.16.148.19/

Activity      State   Last Start  Last Success
------------  ----------------------------
full-transfer Failure
Dell#
EULA: Accepted
Server: default
   Enabled: Yes
   URL: https://stor.g3.ph.dell.com
Service status: Enabled
Server: chennai
   Enabled: Yes
   URL: http://10.16.148.19/

<table>
<thead>
<tr>
<th>Activity</th>
<th>State</th>
<th>Last Start</th>
<th>Last Success</th>
</tr>
</thead>
</table>

Dell#
The commands in this section configure time values on the system, either using the Dell Networking OS, or the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host. For more information, see “Network Time Protocol” of the Management section in the Dell Networking OS Configuration Guide.

The commands in this chapter are generally supported on Dell Networking OS with some exceptions, as notes in the Command History fields.

Topics:

- clock summer-time date
- clock summer-time recurring
- clock timezone
- debug ntp
- ntp authenticate
- ntp authentication-key
- ntp broadcast client
- ntp disable
- ntp multicast client
- ntp master <stratum>
- ntp offset-threshold
- ntp server
- ntp source
- ntp trusted-key
- show clock
- show ntp associations
- show ntp vrf associations
- show ntp status

**clock summer-time date**

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

**Syntax**

clock summer-time time-zone date start-month start-day start-year start-time end-month end-day end-year end-time [offset]

To delete a daylight saving time zone configuration, use the **no clock summer-time** command.

**Parameters**

- **time-zone**
  - Enter the three-letter name for the time zone. This name is displayed in the show clock output.

- **start-month**
  - Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
**start-day**
Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.

**start-year**
Enter a four-digit number as the year. The range is from 1993 to 2035.

**start-time**
Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.

**end-day**
Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.

**end-month**
Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.

**end-time**
Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.

**end-year**
Enter a four-digit number as the year. The range is from 1993 to 2035.

**offset**
(Optional) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is **60 minutes**.

**Defaults**
Not configured.

**Command Modes**
CONFIGURATION

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Related Commands**
- **clock summer-time recurring** — sets a date (and time zone) on which to convert the switch to daylight saving time each year.
- **show clock** — displays the current clock settings.
clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

Syntax

clock summer-time time-zone recurring [start-week start-day start-month start-time end-week end-day end-month end-time [offset]]

To delete a daylight saving time zone configuration, use the no clock summer-time command.

Parameters

time-zone
Enter the three-letter name for the time zone. This name is displayed in the show clock output. You can enter up to eight characters.

start-week
(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for start-day through end-time:

- week-number: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time.
- first: Enter this keyword to start daylight saving time in the first week of the month.
- last: Enter this keyword to start daylight saving time in the last week of the month.

start-day
Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations; for example, Sun, Sat, Mon, and so on. The range is from Sun to Sat.

start-month
Enter the name of one of the 12 months in English.

start-time
Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.

day-week
Enter the one of the following as the week that daylight saving ends:

- week-number: enter a number from 1 to 4 as the number of the week to end daylight saving time.
- first: enter the keyword first to end daylight saving time in the first week of the month.
- last: enter the keyword last to end daylight saving time in the last week of the month.

day-end
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.

day-month
Enter the name of one of the 12 months in English.

day-time
Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.

offset
(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is 60 minutes.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
Version       Description
9.10(0.0)     Introduced on the S6100-ON.
9.8(1.0)      Introduced on the Z9100-ON.
9.8(0.0P5)    Introduced on the S4048-ON.
9.8(0.0P2)    Introduced on the S3048-ON.
9.7(0.0)      Introduced on the S6000-ON.
9.2(1.0)      Introduced on the Z9500.
9.0.2.0       Introduced on the S6000.
8.3.19.0      Introduced on the S4820T.
8.3.11.1      Introduced on the Z9000.
8.3.7.0       Introduced on the S4810.
7.6.1.0       Introduced on the S-Series.
7.5.1.0       Introduced on the C-Series.
7.4.1.0       Updated the start-day and end-day options to allow for using the three-letter abbreviation of the weekday name.
6.1.1.0       Introduced on the E-Series.

Related Commands
• ntp trusted-key — configures a trusted key.
• clock summer-time date — sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.
• show clock — displays the current clock settings.

clock timezone

Configure a timezone for the switch.

Syntax
clock timezone timezone-name offset

To delete a timezone configuration, use the no clock timezone command.

Parameters
timezone-name Enter the name of the timezone. You cannot use spaces.
offset Enter one of the following:
• a number from 1 to 23 as the number of hours in addition to universal time coordinated (UTC) for the timezone.
• a minus sign (-) then a number from 1 to 23 as the number of hours.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
// Table of Version and Description
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.

### debug ntp

Display network time protocol (NTP) transactions and protocol messages for troubleshooting.

**Syntax**

```plaintext
debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}
```

To disable debugging of NTP transactions, use the `no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` command.

**Parameters**

- `adjust`: Enter the keyword `adjust` to display information on NTP clock adjustments.
- `all`: Enter the keyword `all` to display information on all NTP transactions.
- `authentication`: Enter the keyword `authentication` to display information on NTP authentication transactions.
- `events`: Enter the keyword `events` to display information on NTP events.
- `loopfilter`: Enter the keyword `loopfilter` to display information on NTP local clock frequency.
- `packets`: Enter the keyword `packets` to display information on NTP packets.
- `select`: Enter the keyword `select` to display information on the NTP clock selection.
- `sync`: Enter the keyword `sync` to display information on the NTP clock synchronization.

**Command Modes**

- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**ntp authenticate**

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

**Syntax**

```
ntp authenticate
```

To disable NTP authentication, use the `no ntp authentication` command.

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
</tbody>
</table>
### ntp authentication-key

Specify a key for authenticating the NTP server.

**Syntax**

```
ntp authentication-key number md5 [0 | 7] key
```

**Parameters**

- `number`: Specify a number for the authentication key. The range is from 1 to 4294967295. This number must be the same as the `number` parameter configured in the `ntp trusted-key` command.
- `md5`: Specify that the authentication key is encrypted using MD5 encryption algorithm.
- `0`: Specify that authentication key is entered in an unencrypted format (default).
- `7`: Specify that the authentication key is entered in DES encrypted format.
- `key`: Enter the authentication key in the previously specified format.

**Defaults**

NTP authentication is not configured by default. If you do not specify the option `[0 | 7]`, 0 is selected by default.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Added options `[0</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

After configuring the `ntp authentication-key` command, configure the `ntp trusted-key` command to complete NTP authentication.
Dell Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous Dell Networking OS versions; beginning in version 8.2.1.0, Dell Networking OS uses DES encryption to store the key in the startup-config when you enter the `ntp authentication-key` command. Therefore, if your system boots with a startup-configuration from an Dell Networking OS versions prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

### Related Commands
- `ntp authenticate` — enables NTP authentication.
- `ntp trusted-key` — configures a trusted key.

### ntp broadcast client
Set up the interface to receive NTP broadcasts from an NTP server.

**Syntax**
```
ntp broadcast client
```

To disable broadcast, use the `no ntp broadcast client` command.

**Defaults**
Disabled.

**Command Modes**
INTERFACE

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### ntp disable
Prevent an interface from receiving NTP packets.

**Syntax**
```
ntp disable
```
To re-enable NTP on an interface, use the `no ntp disable` command.

**Defaults**

Disabled (that is, if you configure an NTP host, all interfaces receive NTP packets)

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**ntp multicast client**

To receive NTP information from the network via multicast, configure the switch.

**Syntax**

```
ntp multicast client [multicast-address]
```

To disable multicast reception, use the `no ntp multicast client [multicast-address]` command.

**Parameters**

- `multicast-address` (OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in `X::X::X::X` format. If you do not enter a multicast address, the address:
  - `224.0.1.1` is configured if the interface address is IPv4
  - `ff05::1` is configured if the interface address is IPv6

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*. 
**ntp master <stratum>**

Configure the switch as NTP Server.

**Syntax**

```
ntp master <stratum>
```

**Parameters**

- `ntp master <stratum>`
  - Enter the stratum number to identify the NTP Server's hierarchy.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>

**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
```

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
To disable the threshold value, use the `no ntp offset-threshold` command.

**Parameters**

- **offset-threshold**
  - (Optional) Enter the keyword `offset-threshold` and then the threshold value. The range is from 0 to 999.

**Defaults**

Not enabled.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>9.10(0.0)</strong></td>
</tr>
</tbody>
</table>

**Usage Information**

The `ntp offset-threshold` command does not time synchronization.

**Example**

```
Dell(config)# ntp offset-threshold 4
```

### ntp server

Configure an NTP time-serving host.

**Syntax**

```
ntp server[vrf vrf-name] (hostname | ipv4-address | ipv6-address) [key keyid] [prefer] [version number]
```

**Parameters**

- **vrf vrf-name**
  - (Optional) Enter the keyword `vrf` and then the name of the VRF to configure an NTP time-serving host corresponding to that VRF.

- **ipv4-address | ipv6-address**
  - Enter an IPv4 address (A.B.C.D) or IPv6 address (X:XX:XX::X) of NTP server.

- **hostname**
  - Enter the host name of the server.

- **key keyid**
  - (OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. The range is from 1 to 4294967295.

- **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.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>9.8(1.0)</strong></td>
</tr>
<tr>
<td><strong>9.8(0.0P5)</strong></td>
</tr>
</tbody>
</table>
### Usage Information

You can configure multiple time-serving hosts. From these time-serving hosts, the Dell Networking OS chooses one NTP host with which to synchronize. To determine which server is selected, use the `show ntp associations` command.

Because many polls to NTP hosts can affect network performance, Dell Networking recommends limiting the number of hosts configured.

By default, the system performs a time synchronization if the time difference from the time source is greater than one second.

### Related Commands

- `show ntp associations` — displays the NTP servers configured and their status.

### ntp source

Specify an interface's IP address to be included in the NTP packets.

**Syntax**

```
ntp source interface
```

To delete the configuration, use the `no ntp source` command.

**Parameters**

- `interface`

Enter the following keywords and slot/port or number information:

- For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

**Defaults**

Not configured.
ntp trusted-key

Set a key to authenticate the system to which NTP synchronizes.

Syntax
ntp trusted-key number

To delete the key, use the no ntp trusted-key number command.

Parameters

number

Enter a number as the trusted key ID. The range is from 1 to 4294967295.

Defaults
Not configured.

Command Modes
CONFIGURATION

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.5.1.0</td>
<td>Added support for 4-port 40G line cards.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
### show clock

Display the current clock settings.

**Syntax**

```
show clock [detail]
```

**Parameters**

- `detail` (OPTIONAL) Enter the keyword `detail` to view the source information of the clock.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.1.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### 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.
Example

Dell#show clock
11:05:56.949 UTC Thu Oct 25 2001
Dell#

Example (Detail)

Dell# show clock detail
12:18:10.691 UTC Wed Jan 7 2009
Time source is RTC hardware
Summer time starts 02:00:00 UTC Sun Mar 8 2009
Summer time ends 02:00:00 ABC Sun Nov 1 2009
Dell#

Related Commands

- clock summer-time recurring — displays the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

Syntax

show ntp associations

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.1.1.0 Introduced on the E-Series.

Usage Information

The following describes the show ntp associations command shown in the Example below.

Field Description

Field (none) One or more of the following symbols could be displayed:

- * means synchronized to this peer.
- # means almost synchronized to this peer.
Field | Description
--- | ---
remote | Displays the remote IP address of the NTP peer.
ref clock | Displays the IP address of the remote peer’s reference clock.
st | Displays the peer’s stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when | Displays the last time the switch received an NTP packet.
poll | Displays the polling interval (in seconds).
reach | Displays the reachability to the peer (in octal bitstream).
delay | Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset | Displays the relative time of the NTP peer’s clock to the switch clock (in milliseconds).
disp | Displays the dispersion.

Example

```
Dell# show ntp associations
remote      ref clock  st when poll reach delay  offset disp
=============================================================
10.10.120.5 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16         377   -0.08 -1499.9 104.16
172.31.1.33 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
192.200.0.2 0.0.0.0     16 - 256        0 0.00 0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
Dell#
```

Related Commands

- `show ntp status` — displays the current NTP status.

## show ntp vrf associations

Displays the NTP servers configured for the VRF instance `<vrf-name>`.

**Syntax**

```
show ntp [vrf] <vrf-name> associations.
```

**Command Modes**

EXEC

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant **Dell Networking OS Command Line Reference Guide**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.6(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
</tbody>
</table>
show ntp status

Display the current NTP status.

Syntax

    show ntp status

Command Modes

  - EXEC
  - EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0)  Introduced on the S6100–ON.
9.8(1.0)   Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0)   Introduced on the S6000-ON.
9.2(1.0)   Introduced on the Z9500.
9.0.2.0    Introduced on the S6000.
8.3.19.0   Introduced on the S4820T.
8.3.11.1   Introduced on the Z9000.
8.3.7.0    Introduced on the S4810.
7.6.1.0    Introduced on the S-Series.
7.5.1.0    Introduced on the C-Series.
6.1.1.0    Introduced on the E-Series.

Usage Information

The following describes the show ntp status command shown in the Example below.

Field     Description

“Clock is...” States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.

“frequency is...” Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
Field          | Description
-------------|-----------------|
“reference time is...” | Displays the reference time stamp. |
“clock offset is...” | Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock. |
“root dispersion is...” | Displays the root and path dispersion. |
“peer mode is...” | State what NTP mode the switch is. This should be Client mode. |

Example

Dell# show ntp status
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan 10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer dispersion msec
peer mode is client
Dell#

Related Commands

- `show ntp associations` — displays information on the NTP master and peer configurations.
Tunneling is supported on Dell Networking OS.

Topics:
- ip unnumbered
- ipv6 unnumbered
- tunnel allow-remote
- tunnel destination
- tunnel dscp
- tunnel flow-label
- tunnel hop-limit
- tunnel keepalive
- tunnel-mode
- tunnel source

ip unnumbered

Configure a tunnel interface to operate without a unique IPv4 address and select the interface from which the tunnel borrows its address.

Syntax

```
ip unnumbered interface-type
```

To set the tunnel back to default logical address use the `no ip unnumbered` command. If the tunnel was previously operational, the tunnel interface is operationally down unless you also configure the tunnel IPv6 address.

Parameters

- **interface-type**
  
Enter the interface type, followed by a slot/port/subport number.

Defaults

None

Command Modes

INTERFACE TUNNEL

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.1)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z9000.</td>
</tr>
</tbody>
</table>
Version Description
9.3(0.1) Introduced on the S5000 and Z9000.

Usage Information
The ip unnumbered command fails in two conditions:
- If the logical IP address is configured.
- If Tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels, the logical address route information must be present at both the ends.

NOTE: The ip unnumbered command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface is not changed to operationally up until the logical IP address is identified from one of the address family.

ipv6 unnumbered

Configure a tunnel interface to operate without a unique IPv6 address and select the interface from which the tunnel borrows its address.

Syntax
ipv6 unnumbered {interface-type interface-number}

To set the tunnel back to default logical address use the no ipv6 unnumbered command. If the tunnel was previously operational, the tunnel interface is operationally down unless you also configure the tunnel IPv4 address.

Parameters

- interface-type
- interface-number

Enter the interface type, followed by the type, and then the slot/port/subport information.

Defaults
None.

Command Modes
INTERFACE TUNNEL

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.4(0.0) Introduced on the S4810, S4820T.
9.3(0.1) Introduced on the S6000 and Z9000.

Usage Information
The ipv6 unnumbered command fails in two conditions:
- If the logical IP address is configured.
- If Tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels, the logical address route information must be present at both the ends.
NOTE: The ipv6 unnumbered command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface is not changed to operationally up until the logical IP address is identified from one of the address family.

tunnel allow-remote

Configure an IPv4 or IPv6 address or prefix whose tunneled packets are accepted for decapsulation. If you do not configure allow-remote entries, tunneled packets from any remote peer address is accepted.

This feature is supported on Dell Networking OS.

Syntax
tunnel allow-remote {ip-address | ipv6-address} [mask]

To delete a configured allow-remote entry use the no tunnel allow-remote command. Any specified address/mask values must match an existing entry for the delete to succeed. If the address and mask are not specified, this command deletes all allow-remote entries.

Parameters
- **ip-address**
  - Enter the source IPv4 address in A.B.C.D format.

- **ipv6-address**
  - Enter the source IPv6 address in X:X:X:X::X format.

- **mask**
  - (OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D to match a range of remote addresses. The default mask is /32 for IPv4 addresses and /128 for IPv6 addresses, which match only the specified address.

Defaults
If you do not configure tunnel allow remote , all traffic which is destined to tunnel source address is decapsulated.

Command Modes
INTERFACE TUNNEL

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z9000.</td>
</tr>
<tr>
<td>9.3(0.1)</td>
<td>Introduced on the S6000 and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information
You can configure up to eight allow-remote entries on any multipoint receive-only tunnel.

This command fails if the address family entered does not match the outer header address family of the tunnel mode, tunnel source, or any other tunnel allow-remote.

If you configure any allow-remote , the tunnel source or tunnel mode commands fail if the outer header address family does not match that of the configured allow-remote.
**tunnel destination**

Set a destination endpoint for the tunnel.

**Syntax**

```
tunnel destination {ip-address | ipv6-address}
```

To delete a tunnel destination address, use the `no tunnel destination {ip-address | ipv6-address}` command.

**Parameters**

- **ip-address**: Enter the destination IPv4 address for the tunnel.
- **ipv6-address**: Enter the destination IPv6 address for the tunnel.

**Defaults**

none

**Command Modes**

INTERFACE TUNNEL (conf-if-tu)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

The tunnel interface is inoperable without a valid tunnel destination address for the configured Tunnel mode.

To establish a logical tunnel to the particular destination address, use the destination address of the outer tunnel header. If you configure a tunnel interface or source address, the tunnel destination must be compatible.

**tunnel dscp**

Configure the method to set the DSCP in the outer tunnel header.

**C9000 Series**

**Syntax**

```
tunnel dscp {mapped | value}
```

To use the default tunnel mapping behavior, use the `no tunnel dscp value` command.

**Parameters**

- **mapped**: Enter the keyword `mapped` to map the original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.
value

Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of 0 denotes mapping of original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

Defaults

0 (Mapped)

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.9(0.0)</td>
<td>Introduced on the C9010.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S6000, S4810, S4820T, Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

This command configures the method used to set the high 6 bits (the differentiated services codepoint) of the IPv4 TOS or the IPv6 traffic class in the outer IP header.

A value of 0 copies original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

tunnel flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

Syntax

tunnel flow-label value

To return to the default value of 0, use the no tunnel flow-label value command.

Parameters

value

Enter a value to set the IPv6 flow label value in the tunnel header. The range is from 0 to 1048575. The default value is 0.

Defaults

0 (Mapped original packet flow-label value to tunnel header flow-label value)

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
### tunnel hop-limit

Configure the method to set the IPv4 time-to-live or the IPv6 hop limit value in the outer tunnel header.

**Syntax**

```plaintext
tunnel hop-limit
```

To restore the default tunnel hop-limit, use the `no tunnel hop-limit` command.

**Parameters**

- **value**
  
  Enter the hop limit (ipv6) or time-to-live (ipv4) value to include in the tunnel header. The range is from 0 to 255. The default is 64.

**Defaults**

64 (Time-to-live for IPv4 outer tunnel header or hop limit for IPv6 outer tunnel header)

**Command Modes**

INTERFACE TUNNEL (conf-if-tu)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S6000, S4810, S4820T, Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

A value of 0 copies the inner packet hop limit (ipv6) or time-to-live (ipv4) in the encapsulated packet to the tunnel header hop limit (ipv6) or time-to-live (ipv4) value.

### tunnel keepalive

Configure the tunnel keepalive target, interval and attempts.

**Syntax**

```plaintext
tunnel keepalive {ip-address | ipv6-address}[interval {seconds}] [attempts {count | unlimited}]
```

To disable the tunnel keepalive probes use the `no tunnel keepalive` command.
Parameters

- **ip-address ipv6 address**
  Enter the IPv4 or IPv6 address of the peer to which the keepalive probes will be sent.

- **interval seconds**
  Enter the keyword interval then the interval time, in seconds, after which the restart process to keepalive probe packets.
  The range is from 5 to 255. The default is 5.

- **count**
  (OPTIONAL) Enter the keyword count to count packets processed by the filter.
  The range is from 3 to 10. The default is 3.

- **unlimited**
  Enter the keyword unlimited to specify the unlimited number of keepalive probe packets.

Defaults
Tunnel keepalive is disabled.

Command Modes
INTERFACE TUNNEL

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information
Enabling tunnel keepalive causes ICMP echo packets to be sent to the keepalive target. The ICMP echo will be sourced from the tunnel interface logical IPv4 or IPv6 address and will be tunnel encapsulated. The response will be accepted whether it returns tunnel encapsulated or not.

When configuring tunnel keepalive at both end points of a tunnel interface it is recommended to set the tunnel keepalive target to the logical IPv4 or IPv6 address of the far end tunnel peer, rather than to the tunnel destination. This reduces the chance of both ends of the tunnel staying in keepalive down state. If both ends get into a keepalive down state that does not clear in a few seconds, then performing shutdown - no shutdown sequence on one end should bring both ends back to up.

tunnel-mode

Enable a tunnel interface.

Syntax
tunnel mode {ipip | ipv6 | ipv6ip}[decapsulate-any]
To disable an active tunnel interface, use the `no tunnel mode` command.

### Parameters

- **ipip**
  - Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.

- **ipv6**
  - Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.

- **ipv6ip**
  - Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.

- **decapsulate-any**
  - (Optional) Enable tunnel in multipoint receive-only mode.

### Defaults

There is no default tunnel mode.

### Command Modes

- INTERFACE TUNNEL

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the decapsulate-any command.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S6000 and Z9000.</td>
</tr>
</tbody>
</table>

### 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.

- **Syntax**
  ```
  tunnel source {ip-address | ipv6-address | interface-type-number | anylocal}
  ```

  To delete the current tunnel source address, use the `no tunnel source` command.

- **Parameters**
  - **ip-address**
    - Enter the source IPv4 address in A.B.C.D format.
  - **ipv6-address**
    - Enter the source IPv6 address in X::X::X::X format.
For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.

For a VLAN interface, enter the keyword vlan then a number from 1 to 4094.

For a port-channel interface, enter the keywords port-channel then the port-channel ID.

Enter the anylocal command to allow the multipoint receive-only tunnel to decapsulate tunnel packets destined to any local ip address.

Defaults

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the tunnel source anylocal command.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000 and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

Added an optional keyword “anylocal” to the tunnel source command. The anylocal argument can be used in place of the ip address or interface, but only with the multipoint receive-only mode tunnels. The tunnel source anylocal command allows the multipoint receive-only tunnel to decapsulate tunnel packets addressed to any IPv4 or IPv6 (depending on the tunnel mode) address configured on the switch that is operationally Up.
Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with NIC teaming, automatic recovery from a failed link.

Topics:
- clear ufd-disable
- debug uplink-state-group
- description
- downstream
- downstream auto-recover
- downstream disable links
- enable
- show running-config uplink-state-group
- show uplink-state-group
- uplink-state-group
- upstream

**clear ufd-disable**

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

**Syntax**

```
clear ufd-disable {interface interface | uplink-state-group group-id}
```

**Parameters**

- **interface interface**: Specify one or more downstream interfaces. For `interface`, enter one of the following interface types:
  - 1 Gigabit Ethernet: `gigabitethernet {slot/port | slot/port-range}`
  - 10 Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
  - Port channel: `port-channel {1–128 | 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: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

- **uplink-state-group group-id**: Re-enables all UFD-disabled downstream interfaces in the group. The valid `group-id` values are from 1 to 16.

**Defaults**

A downstream interface in a UFD-disabled uplink-state group is also disabled and is in a UFD-Disabled Error state.

**Command Modes**

CONFIGURATION
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.3</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>

### 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.

#### S3048-ON

**Syntax**

```plaintext
debug uplink-state-group [group-id]
```

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

**Parameters**

- `group-id` Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.

**Defaults**

none

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Version Description

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.3</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>
Related Commands

- `clear ufd-disable` — re-enable downstream interfaces that are in a UFD-Disabled Error state.

**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

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 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.
- 9.2(0.0)
  - Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
- 8.3.19.0
  - Introduced on the S4820T.
- 8.3.12.0
  - Introduced on the S4810.
- 8.4.2.3
  - Introduced on the S-Series S50.

**Example**

```bash
Dell(conf-uplink-state-group-16)# description test
Dell(conf-uplink-state-group-16)#
```

**Related Commands**

- `uplink-state-group` — create 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:
  - 1 Gigabit Ethernet: `gigabitethernet {slot/port | slot/port-range}`
  - 10 Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
  - Port channel: `port-channel {1-128 | 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:
gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5. A comma is required to separate each port and port-range entry.

**Defaults**
none

**Command Modes**
UPLINK-STATE-GROUP

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(2.3)</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>

**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

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
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
- `number`: Enter the number of downstream links the UFD brings down. The range is from 1 to 1024.
- `all`: Brings down all downstream links in the group.

Defaults
No downstream links are disabled when an upstream link in an uplink-state group goes down.

Command Modes
- UPLINK-STATE-GROUP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
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.
9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.
8.4.2.3 Introduced on the S-Series S50.

Usage Information
When one upstream interface in an uplink-state group goes down, you can configure the number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message.
If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

Related Commands

- **downstream** — assigns a port or port-channel to the uplink-state group as a downstream interface.
- **uplink-state-group** — creates an uplink-state group and enables the tracking of upstream links.

**enable**

Enable uplink state group tracking for a specific UFD group.

**Syntax**

```
enable
```

**Defaults**

Upstream-link tracking is automatically enabled in an uplink-state group.

**Command Modes**

UPLINK-STATE-GROUP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4(2.3)</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>

**Related Commands**

- **uplink-state-group** — create an uplink-state group and enables the tracking of upstream links.

**show running-config uplink-state-group**

Display the current configuration of one or more uplink-state groups.

**Syntax**

```
show running-config uplink-state-group [group-id]
```

**Parameters**

- **group-id**

  Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are from 1 to 16.

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.3</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>

Example

Dell# show running-config uplink-state-group
!
no enable
uplink state track 1
downstream GigabitEthernet 1/2,4,6,11-19
upstream TengigabitEthernet 1/49, 50
upstream PortChannel 1
!
uplink state track 2
downstream GigabitEthernet 1/1,3,5,7-10
upstream TengigabitEthernet 1/51,52

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**

- `group-id` Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
- `detail` Displays additional status information on the upstream and downstream interfaces in each group

**Defaults**

none

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
u**plink-state-group**

Create an uplink-state group and enable the tracking of upstream links on a switch or router.

**Syntax**

```
uplink-state-group group-id
```

**Example**

Dell# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface disabled
Uplink State Group : 1 Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 3 Status: Enabled, Up
Upstream Interfaces : Gi 1/25(Up) Gi 1/28(Up)
Downstream Interfaces : Te 5/1(Up) Te 5/1(Up) Te 5/3(Up) Te 5/5(Up) Te 5/6(Up)
Uplink State Group : 5 Status: Enabled, Down
Upstream Interfaces : Gi 1/1(Dwn) Gi 1/3(Dwn) Gi 1/5(Dwn)
Downstream Interfaces : Te 5/2(Dis) Te 5/4(Dis) Te 5/11(Dis) Te 5/12(Dis) Te 5/13(Dis) Te 5/14(Dis) Te 5/15(Dis)
Uplink State Group : 6 Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 7 Status: Enabled, Up
Upstream Interfaces :
Downstream Interfaces :
Uplink State Group : 16 Status: Disabled, Up
Upstream Interfaces : Gi 1/25(Dwn) Po 8(Dwn)
Downstream Interfaces : Gi 1/30(Dwn)

**Related Commands**

- `show running-config uplink-state-group` — displays the current configuration of one or more uplink-state groups.
- `uplink-state-group` — creates an uplink-state group and enables the tracking of upstream links.
To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

**Parameters**

- **group-id**: Enter the ID number of an uplink-state group. The range is from 1 to 16.

**Defaults**

- none

**Command Modes**

- CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.2.3</td>
<td>Introduced on the S-Series S50.</td>
</tr>
</tbody>
</table>

**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 operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered 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
Dell(conf)#
```

**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.
Enter one of the following interface types:

- 1 Gigabit Ethernet: `gigabitethernet {slot/port | slot/port-range}`
- 10 Gigabit Ethernet: `tengigabitethernet {slot/port | slot/port-range}`
- Port channel: `port-channel {1-128 | 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: `gigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

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 gigabitethernet 1/10-15
Dell(conf-uplink-state-group-16)#
```
VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can “stack” VLANs into one tunnel and switch them through the network transparently.

The Dell Networking OS supports this feature.

For more information about basic VLAN commands, see the Virtual LAN (VLAN) Commands section in Layer 2.

Important Points to Remember

- If you do not enable the spanning tree protocol (STP) across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer’s networks are tunneled across the stackable VLAN network.
- If you do enable STP across the stackable VLAN network, STP BPDUs from the customer’s networks are consumed and not tunneled across the stackable VLAN network unless you enable protocol tunneling.

**NOTE:** For more information about protocol tunneling on the E-Series, see Service Provider Bridging.

- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN are not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) management over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- Dell Networking recommends that you do not use the same MAC address, on different customer VLANs, on the same stackable VLAN.
- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands do not switch traffic for the default VLAN. These interfaces are switch traffic only when they are added to a non-default VLAN.
- Starting with Dell Networking OS version 7.8.1 for C-Series and S-Series (Dell Networking OS version 7.7.1 for E-Series, 8.2.1.0 for E-Series ExaScale), a vlan-stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the vlan-stack trunk port is also a member of an untagged vlan, the port must be in Hybrid mode. For more information, see portmode hybrid.

Topics:

- dei honor
- dei mark
- member
- stack-unit stack-group
- vlan-stack access
- vlan-stack compatible
- vlan-stack dot1p-mapping
- vlan-stack protocol-type
- vlan-stack trunk

**dei honor**

Honor the incoming DEI value by mapping it to a Dell Networking OS drop precedence. Enter the command once for 0 and once for 1.

**Syntax**

dei honor \{0 | 1\} \{green | red | yellow\}
Parameters

0 | 1 Enter the bit value you want to map to a color.

green | red | yellow Choose a color:
  - Green: High priority packets that are the least preferred to be dropped.
  - Yellow: Lower priority packets that are treated as best-effort.
  - Red: Lowest priority packets that are always dropped (regardless of congestion status).

Defaults

Disabled; Packets with an unmapped DEI value are colored green.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

Enable DEI before using this command.

dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

**S3048–ON**

Syntax
dei mark {green | yellow} {0 | 1}

Parameters

0 | 1 Enter the bit value you want to map to a color.

green | red | yellow Choose a color:
  - Green: High priority packets that are the least preferred to be dropped.
  - Yellow: Lower priority packets that are treated as best-effort.

Defaults

All the packets on egress are marked with DEI 0.
**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

Enable DEI before using this command.

**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 the interface information:
  - For a Port Channel interface, enter the keywords `port-channel`, and then a number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

**Defaults**

Not configured.

**Command Modes**

CONF-IF-VLAN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
</tbody>
</table>
VLAN Stacking

Usage Information

Enable the stackable VLAN (using the vlan-stack compatible command) on the VLAN prior to adding a member to the VLAN.

Related Commands

- vlan-stack compatible — enables stackable VLAN on a VLAN.

stack-unit stack-group

Configure a stacking group specified by an ID.

Syntax

[no] stack-unit unit-id stack-group stack-group-id

To remove the current stack group configuration, use the no stack-unit unit-id stack-group stack-group-id command.

Parameters

- **unit-id**: Enter the stack unit ID.
- **stack-group-id**: Enter the stack group ID. The range is from 0 to 16.

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.
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 Z9000.
9.0.2.0 | Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.10.2 | Introduced on the S4810.
Usage Information

⚠️ **WARNING:** The following message displays to confirm the command: All non-default configurations on the related member ports ports (<ports listed here>) will be removed. Do you want to continue (y/n)? If you enter “y”, all non-default configurations on any member ports of the current stack group are removed when you reboot the unit.

## vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

**Syntax**

```plaintext
vlan-stack access
```

To remove access port designation, use the `no vlan-stack access` command.

**Defaults**

Not configured.

**Command Modes**

`INTERFACE`

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**E-Series original Command**

**Usage Information**

Prior to enabling this command, to place the interface in Layer 2 mode, enter the `switchport` command.

To remove the access port designation, remove the port (using the `no member interface command`) from all stackable VLAN-enabled VLANs.

## vlan-stack compatible

Enable the stackable VLAN feature on a VLAN.

**Syntax**

```plaintext
vlan-stack compatible
```

1546 | VLAN Stacking
To disable the Stackable VLAN feature on a VLAN, use the `no vlan-stack compatible` command.

**Defaults**
Not configured.

**Command Modes**
CONF-IF-VLAN

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
Prior to disabling the stackable VLAN feature, remove the members.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

If you enabled VRF, you cannot enable the stacked VLAN feature using this command.

If you enabled IGMP snooping, you cannot enable the stacked VLAN feature using this command.

**Example**
Dell# show vlan

Codes: * - Default VLAN, G - GVRP VLANs

```
  NUM  Status    Q Ports
    1    Inactive  M Gi 1/13
    2    Active    M Gi 1/1-3
    3    Active    M Po1(Gi 1/14-15)
           M Gi 1/18
           M Gi 1/4
    4    Active    M Po1(Gi 1/14-15)
           M Gi 1/18
           M Gi 1/5
    5    Active    M Po1(Gi 1/14-15)
           M Gi 1/18
           M Gi 1/6
```

Dell#
**vlan-stack dot1p-mapping**

Map C-Tag dot1p values to an S-Tag dot1p value.

**Syntax**

```
vlan-stack dot1p-mapping c-tag-dot1p values sp-tag-dot1p value
```

**Parameters**

- `c-tag-dot1p value`
  - Enter the keyword `c-tag-dot1p` then the customer dot1p value that is mapped to a service provider dot1p value. The range is from 0 to 7.

- `sp-tag-dot1p value`
  - Enter the keyword `sp-tag-dot1p` then the service provider dot1p value. The range is from 0 to 7.

**Defaults**

none

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

You can separate the C-Tag values by commas or dashed ranges. In the case of conflicts, dynamic mode CoS overrides any Layer 2 QoS configuration.

**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 Dell Networking OS 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

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the E-Series. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.</td>
</tr>
<tr>
<td>8.2(1.0)</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td>7.6(1.0)</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Usage Information

For specific interoperability limitations regarding the S-Tag TPID, see the Dell Networking OS Configuration Guide.

The four characters you may enter are shown in the following table.

<table>
<thead>
<tr>
<th>Number</th>
<th>Resulting TPID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0x0001</td>
</tr>
<tr>
<td>10</td>
<td>0x0010</td>
</tr>
<tr>
<td>81</td>
<td>0x0081</td>
</tr>
<tr>
<td>8100</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

Related Commands

- portmode hybrid — sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.
- vlan-stack trunk — specifies a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

**vlan-stack trunk**

Specify a Layer 2 port or port channel as a trunk port to the stackable VLAN network.

**Syntax**

```
vlan-stack trunk
```

To remove a trunk port designation from the selected interface, use the `no vlan-stack trunk` command.

**Defaults**

Not configured.
command modes:

- INTERFACE

command history:

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.2.1.0</td>
<td>Introduced on the E-Series.</td>
</tr>
<tr>
<td></td>
<td>C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.</td>
</tr>
<tr>
<td>7.8.1.0</td>
<td>Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port.</td>
</tr>
<tr>
<td>7.7.1.0</td>
<td>Functionality augmented for E-Series to enable multi-purpose use of the port.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the C-Series and S-Series.</td>
</tr>
</tbody>
</table>

Usage Information:

Prior to using this command, to place the interface in Layer 2 mode, use 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.

In Example 1, a VLAN-Stack trunk port is configured and then made part of a single-tagged VLAN.

In Example 2, the tag protocol identifier (TPID) is set to 88A8. The Gi 3/10 port is configured to act as a VLAN-Stack access port; the Gi 5/1 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, you need the native VLAN feature. Use the portmode hybrid command. For more information, see the portmode hybrid command.

Example 1:

```
Dell(conf-if-gi-1/42)# switchport
Dell(conf-if-gi-1/42)# vlan-stack trunk
Dell(conf-if-gi-1/42)# show config

interface GigabitEthernet 1/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
Dell(conf-if-gi-1/42)# interface vlan 100
Dell(conf-if-vl-100)# vlan-stack compatible
Dell(conf-if-vl-100-stack)# member gigabitethernet 1/42
Dell(conf-if-vl-100-stack)# show config
```
interface Vlan 100
  no ip address
  vlan-stack compatible
  member GigabitEthernet 1/42
  shutdown
Dell(conf-if-vl-100-stack)# interface vlan 20
Dell(conf-if-vl-20)# tagged gigabitethernet 1/42
Dell(conf-if-vl-20)# show config

interface Vlan 20
  no ip address
  tagged GigabitEthernet 1/42
  shutdown
Dell(conf-if-vl-20)# do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
  x - Dot1x untagged, X - Dot1x tagged
  G - GVRP tagged, M - Vlan-stack

<table>
<thead>
<tr>
<th>NUM</th>
<th>Status</th>
<th>Description</th>
<th>Q</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Active</td>
<td></td>
<td>T</td>
<td>Gi 1/42</td>
</tr>
<tr>
<td>100</td>
<td>Active</td>
<td></td>
<td>M</td>
<td>Gi 1/42</td>
</tr>
</tbody>
</table>
Dell(conf-if-vl-20)#

Example 2

Dell(config)# vlan-stack protocol-type 88A8
Dell(config)# interface gigabitethernet 3/10
Dell(config-if-gi-3/10)# no shutdown
Dell(config-if-gi-3/10)# switchport
Dell(config-if-gi-3/10)# vlan-stack access
Dell(config-if-gi-3/10)# exit

Dell(config)# interface gigabitethernet 5/1
Dell(config-if-gi-5/1)# no shutdown
Dell(config-if-gi-5/1)# portmode hybrid
Dell(config-if-gi-5/1)# switchport
Dell(config-if-gi-5/1)# vlan-stack trunk
Dell(config-if-gi-5/1)# exit

Dell(config)# interface vlan 10
Dell(config-if-vlan)# vlan-stack compatible
Dell(config-if-vlan)# member Gi 4/1, Gi 3/10, Gi 5/1
Dell(config-if-vlan)# exit

Dell(config)# interface vlan 30
Dell(config-if-vlan)# untagged Gi 5/1
Dell(config-if-vlan)# exit
Dell(config)#

Dell(config)# interface vlan 40
Dell(config-if-vlan)# tagged Gi 5/1
Dell(config-if-vlan)# exit
Dell(config)#
Virtual Routing and Forwarding (VRF)

Virtual routing and forwarding (VRF) allows multiple instances of a routing table to coexist on the same router at the same time.

Topics:
- ip vrf
- ip http vrf
- description
- ip vrf forwarding
- ip route-export
- ip route-import
- ipv6 route-export
- ipv6 route-import
- match source-protocol
- redistribute
- interface management
- maximum dynamic-routes
- show ip vrf
- show run vrf

ip vrf

Create or delete a customer VRF.

Syntax

```
ip vrf {vrf-name | management} [vrf_id]
```  
To delete a customer VRF, use the no ip vrf {vrf-name | management} [vrf_id] command.

Parameters

- **vrf-name**: Enter the name of the VRF that you create.
- **management**: Enter the keyword management to create the management VRF.
- **vrf_id**: (Optional) Enter the ID of the VRF that you create.

Defaults

Available by default for management VRF. For creating other customer VRFs, enable the feature vrf option in Configuration mode.

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.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
ip http vrf

Configure an HTTP client with a VRF used to connect to the HTTP server.

Syntax

ip http vrf {management | vrf-name}

To undo the HTTP client configuration, use the ip http vrf command.

Parameters

management Enter the keyword management for configuring the management VRF that uses an HTTP client.

vrf-name Enter a VRF name that the HTTP client uses. If you do not specify a VRF name, the HTTP client uses the default VRF.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.8(0.0) Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information

To make the HTTP clients VRF-aware, use the ip http vrf command. The HTTP client uses the VRF name that you specify to reach the HTTP server. If you do not specify a VRF name, the HTTP client uses the default VRF.
**description**

Specify a name for a customer VRF.

**Syntax**

description string

To delete the descriptive name for a customer VRF, use the no description string command.

**Parameters**

string

Enter a descriptive name for the VRF.

**Defaults**

None.

**Command Modes**

VRF MODE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series.</td>
</tr>
</tbody>
</table>

**ip vrf forwarding**

Attach an interface to a VRF.

**Syntax**

ip vrf forwarding {vrf-name | management}

To delete an interface associated with a configured VRF, use the no ip vrf forwarding {vrf-name | management} command.

**Parameters**

vrf-name

Enter name of the VRF that you want to associate the interface to.

management

Enter the keyword management to associate an interface to the management VRF.

**Defaults**

none

**Command Modes**

INTERFACE-CONFIG

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
</tbody>
</table>
### Version | Description
---|---
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON and Z9500.
9.4.(0.0) | Introduced on the S-Series and Z9000.

#### Usage Information

You can attach an interface to either a nondefault VRF or a management VRF.

To assign a port-back to a default VRF, remove the VRF association from the interface. You can use this only if there is no IP address configured on the interface.

There must be no prior Layer 3 configuration on the interface when configuring VRF.

You must enable VRF before using this command.

You can configure an IP subnet or address on a physical or VLAN interface that overlaps the same IP subnet or address configured on another interface only if the interfaces are assigned to different VRFs. If you assign two interfaces to the same VRF, you cannot configure overlapping IP subnets or the same IP address to them.

#### Example

```
Dell# configure terminal
Dell(conf)# ip vrf red
Dell(conf-vrf)# description "Red Network"
Dell(conf-vrf)# show config
!
ip vrf red 4
description "Red Network"
Dell(conf-vrf)#

Dell(conf-if-gi-1/45)# int gi 1/46
Dell(conf-if-gi-1/46)# no shut
Dell(conf-if-gi-1/46)# ip vrf forwarding red
Dell(conf-if-gi-1/46)# ip add 100.1.1.1/24
Dell(conf-if-gi-1/46)#
Dell(conf-if-gi-1/46)#
Dell(conf-if-gi-1/46)#
Dell(conf-if-gi-1/46)# show config
!
interface GigabitEthernet 1/46
  ip vrf forwarding red
  ip address 100.1.1.1/24
  no shutdown
Dell(conf-if-gi-1/46)#
```

---

**ip route-export**

Enables route leaking between VRFs. This command exports or shares IPv4 routes corresponding to one VRF with other nondefault VRFs.

**Syntax**

```
ip route-export tag [route-map-name]
```

**Parameters**

- **route-export**
  
  Enter the keywords `route-export` to leak or share routes between VRFs.

- **tag**
  
  Enter a tag (export route target) to expose routes to other VRFs. This tag acts as an identifier for exported routes. Use this identifier while importing these routes into another nondefault VRF.

- **route-map-name**
  
  (Optional) Enter the name of the route-map to filter the exported routes.
You can leak global routes to VRFs. As the global RTM usually contains a large pool of routes, when the destination VRF imports global routes, these routes are duplicated into the VRF's RTM. It is mandatory to use route-maps to filter out leaked routes while sharing global routes with VRFs.

**Command Modes**
- VRP mode
- CONFIGURATION mode

**Command History**
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048–ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048–ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.</td>
</tr>
</tbody>
</table>

**Usage Information**
To export all the routes corresponding to a source VRF, you can use the `ip route-export tag` command without specifying the route-map attribute. This action exposes source VRF routes to various other VRFs, which then import these routes using the `ip route-import tag` command.

In Dell Networking OS, you can configure one route-export per VRF as you can only expose one set of routes for leaking. However, you can configure multiple route-import targets because a VRF can accept routes from multiple VRFs.

You can expose a unique set of routes from the source VRF for leaking to other VRFs. When two VRFs leak or export routes, there is no option to discretely filter leaked routes from each source VRF. For example, you cannot import one set of routes from one VRF and another set of routes from another VRF.

Only active routes are eligible for leaking. For example, if one VRF has two routes corresponding to BGP and OSPF, in which the BGP route is not active, the OSPF route takes precedence over BGP. Even though the target VRF has specified filtering options to match BGP, the BGP route is not leaked as that route is not active in the Source VRF.

**Related Commands**
- `ip route-import` — imports routes from another VRF.

### `ip route-import`

Imports IPv4 routes that another VRF leaks using the VRF tag during the export of these routes.

**Syntax**
```
ip route-import tag [route-map-name]
```

**Parameters**
- `route-import`
- `tag`
  - Enter the keywords `route-import` to import routes into the VRF.
  - Enter a tag (ASN number) to specify an import route target for importing routes from another VRF.
  - To import leaked routes from another VRF, use the same ASN number that is specified as the export route target at the source VRF.
route-map-name

Enter the name of the route-map to filter the imported routes.

NOTE: Use the route-map attribute while importing routes from the global RTM. Route-maps allow you to filter routes at the import end based on the matching criteria that you define in the route-map.

Command Modes

• CONFIGURATION
• VRF mode

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.</td>
</tr>
</tbody>
</table>

Usage Information

It is possible to configure multiple import conditions per VRF depending on the exporting VRF. The export-target and import-target support only the match protocol and match prefix-list options. Other options that are configured in the route-maps are ignored.

Related Commands

• ip route-export — exports routes to another VRF.

ipv6 route-export

Enables route leaking between VRFs. This command exports or shares IPv6 routes corresponding to one VRF with other nondefault VRFs.

Syntax

ipv6 route-export tag [route-map-name]

Parameters

route-export

Enter the keywords route-export to leak or share routes between VRFs.

tag

Enter a tag (ASN number) as the export route target to expose routes to other VRFs. This tag acts as an identifier for exported routes. Use this identifier while importing these routes into another nondefault VRF.

route-map-name

(Optional) Enter the name of the route-map to filter the exported routes. You can leak global routes to be made available to VRFs. As the global RTM usually contains a large pool of routes, when the destination VRF imports global routes, these routes are duplicated into the VRF’s RTM. It is mandatory to use route-maps to filter out leaked routes while sharing global routes with VRFs.

Defaults

N/A

Command Modes

• VRF mode
• CONFIGURATION mode
Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.</td>
</tr>
</tbody>
</table>

Usage Information

To export all the routes corresponding to a source VRF, use the `ip route-export tag` command without specifying the route-map attribute. This action exposes source VRF routes to other VRFs, which then import these routes using the `ip route-import tag` command.

In Dell Networking OS, you can configure one route-export per VRF as you can only expose one set of routes for leaking. However, you can configure multiple route-import targets because a VRF can accept routes from multiple VRFs.

You can expose a unique set of routes from the source VRF for leaking to other VRFs. When two VRFs leak or export routes, there is no option to discretely filter leaked routes from each source VRF. For example, you cannot import one set of routes from one VRF and another set of routes from another VRF.

Only active routes are eligible for leaking. For example, if one VRF has two routes corresponding to BGP and OSPF, in which the BGP route is not active, the OSPF route takes precedence over BGP. Even though the target VRF has specified filtering options to match BGP, the BGP route is not leaked as that route is not active in the source VRF.

Related Commands

- `ipv6 route-import` — imports IPv6 routes from another VRF.

**ipv6 route-import**

Imports IPv6 routes that another VRF leaks using the tag that VRF specifies during export of these routes.

**Syntax**

```
ipv6 route-import tag [route-map-name]
```

**Parameters**

- `route-import` Enter the keywords route-import to import IPv6 routes into the VRF.
- `tag` Enter a tag (ASN number) to specify an import route target for importing routes from another VRF. To import leaked routes from another VRF, use the same ASN number that is specified as the export route target at the source VRF.
- `route-map-name` Enter the name of the route-map to filter the imported routes.

**Defaults**

N/A

**Command Modes**

- VRF mode
- CONFIGURATION mode

**Usage Information**

NOTE: Use the route-map attribute while importing routes from the global RTM. Route-maps allow you to filter routes at the import end based on the matching criteria that you define in the route-map.
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.</td>
</tr>
</tbody>
</table>

It is possible to configure multiple import conditions per VRF depending on the exporting VRF.

The export-target and import-target support only the match the protocol and prefix-list options. Other options that you configure in the route-maps are ignored.

Related Commands
- **ipv6 route-export** — exports IPv6 routes to another VRF.

**match source-protocol**

Specify matching source-protocol criteria while exporting or importing routes.

**Syntax**

```
match source-protocol {bgp | isis | ospf | connected | static}
```

**Parameters**

- **bgp**
  - Enter the keyword `bgp` to leak or share routes corresponding to the BGP protocol.
- **isis**
  - Enter the keyword `isis` to leak or share routes corresponding to the ISIS protocol.
- **ospf**
  - Enter the keyword `ospf` to leak or share routes corresponding to the OSPF protocol.
- **connected**
  - Enter the keyword `connected` to leak or share connected routes corresponding to the VRF.
- **static**
  - Enter the keyword `static` to leak or share static routes corresponding to the VRF.

**Command Modes**

ROUTE MAP MODE

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.</td>
</tr>
</tbody>
</table>
Usage Information

Specify the matching criteria only after defining a route-map. Before using this command, you must enter Route Map mode using the `route-map` command. The match criteria that you specify is associated with the route-map that you define.

The export-target and import-target options support only the match protocol and match prefix-list options. Other options that you configure in the route-maps are ignored.

Related Commands

- `ipv6 route-import` — imports IPv6 routes from another VRF.

redistribute

Redistributes leaked or exported routes corresponding to specific protocols.

Syntax

```
redistribute {imported-bgp | import-ospf | import-isis}
```

Parameters

- `imported-bgp` Enter the keywords `imported-bgp` to redistribute leaked routes that are learned using the BGP protocol.
- `imported-ospf` Enter the keywords `imported-ospf` to redistribute leaked routes that are learned using the OSPF protocol.
- `imported-isis` Enter the keywords `imported-isis` to redistribute leaked routes that are learned using the ISIS protocol.
- `route-map` Enter the name of the route-map to specify the filtering criteria for imported routes.

Command Modes

`CONFIGURATION`

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.</td>
</tr>
</tbody>
</table>

Related Commands

- `ip route-import` — import routes from another VRF.

interface management

Associates a management port with a management VRF.

Syntax

```
interface management
```

To delete the association between a management port and a management VRF, use the `no interface management` command.
maximum dynamic-routes

Specify the maximum number of dynamic (protocol) routes a VRF can have.

Syntax
maximum dynamic-routes limit {warn-threshold threshold-value | warning-only}

To remove the limit on the maximum number of routes used, use the no maximum dynamic-routes command.

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit</td>
<td>Maximum number of routes allowed in a VRF. The valid range is from 1 to 16,000 (or maximum allowable for that platform if a smaller value).</td>
</tr>
<tr>
<td>warning-threshold</td>
<td>The warning threshold value is a percentage of the limit value. When the number of routes reaches the specified percentage of the limit, a warning message appears. The valid range is from 1 to 100. After the limit is reached, additional dynamic routes are not allowed.</td>
</tr>
<tr>
<td>warning-only</td>
<td>When you use the warning-only option, when the maximum number of dynamic routes reaches the limit, a warning message appears. After the limit is reached, additional dynamic routes are still allowed.</td>
</tr>
</tbody>
</table>

Defaults
No limit is set on the maximum number of dynamic routes for a VRF.

Command Modes
CONFIGURATION-VRF

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
</tbody>
</table>
### show ip vrf

Displays information corresponding to the VRFs that you configure in the system.

**Syntax**

```plaintext
show ip [vrf vrf-name]
```

**Parameters**

- `vrf vrf-name` Enter the keyword `vrf` then the name of the VRF to display information corresponding to that VRF.

**Command Modes**

- EXEC
- EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S-Series and Z9000.</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
Dell# show ip vrf
VRF-Name       VRF-ID Interfaces
fault           0       Gi 1/1-13,18-47,    
                Te 1/49,50,51,52,    
                Ma 1/1,               
                Ma 2/1,               
                Ma 3/1,               
                Ma 4/1,               
                Ma 5/1,               
                Ma 6/1,               
                Nu 0,                 
                test1
                1       Gi 1/14,16-17
```

Usage Information

If you do not specify the maximum route limit for a VRF, the VRF has unlimited space that extends to the maximum number of entries allowed for the system.
show run vrf

Displays configuration information corresponding to all the VRFs in the system.

Syntax

show run vrf vrf-name

Parameters

- **vrf vrf-name**: Enter the keyword vrf and then the name of the VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

- **Version**
  - 9.10(0.0): Introduced on the S6100-ON.
  - 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 and Z9500.
  - 9.4.(0.0): Introduced on the S-Series and Z9000.

Usage Information

This command displays information from the running-config corresponding to either a specific VRF or all the VRFs in the system.

Example

```
Dell# show run vrf test3
!
ip vrf test3
description "Banking Customer Chennai"
Dell#
```
VLT Proxy Gateway

The virtual link trucking (VLT) proxy gateway feature allows a VLT domain to locally terminate and route L3 packets that are destined to a Layer 3 (L3) endpoint in another VLT domain. Enable the VLT proxy gateway using the link layer discover protocol (LLDP) method or the static configuration. For more information, see the Dell Networking OS Command Line Reference Guide.

Topics:
- proxy-gateway lldp
- proxy-gateway static
- remote-mac-address exclude-vlan
- peer-domain-link port-channel exclude-vlan
- proxy-gateway peer-timeout
- vlt-peer-mac transmit
- show vlt-proxy-gateway

proxy-gateway lldp
Enables the proxy-gateway feature using the LLDP protocol.

S3048–ON

Syntax

[no] proxy-gateway lldp

Command Modes VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048–ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048–ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000–ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

The configuration is cached and sent to LLDP only in one of the following conditions:

1. The port-channel connecting the two VLT domains, across the DC, is a VLT LAG.
2. The protocol lldp command is globally enabled.
3. The proxy-gateway LLDP configuration is applied.
proxy-gateway static

Enables the proxy-gateway feature using static configurations.

S3048–ON

Syntax

[no] proxy-gateway static

Command Modes

VLT DOMAIN

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.
9.8(1.0) | Introduced on the Z9100–ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.4(0.0) | Introduced on the S4810, S4820T, S6000, Z9000.

Usage Information

When you add a proxy-gateway static configuration, the setting is saved in the Layer 2 module. When you remove the static proxy gateway configuration, each proxy-gateway static MAC configured is deleted from the Layer 2 module.

Example

Dell(conf)# vlt-domain 1
Dell(conf-vlt-domain)# proxy-gateway lldp
Dell(conf-vlt-domain)#

remote-mac-address exclude-vlan

Configure the proxy-gateway static entry and exclude a VLAN or a range of VLANs from proxy routing.

S3048–ON

Syntax

[no] remote-mac-address mac-address [exclude-vlan vlan-range]

Parameters

remote-mac-address | Specify the mac-addresses of the VLT peers which are in the remote VLT domain.

mac-address | Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
Enter the VLAN IDs in which proxy gateway is not needed. The VLANs are excluded from doing proxy gateway. The value can be a single VLAN ID, comma-separated VLAN IDs, a range of VLAN IDs, or a combination. For example:

Comma-separated: 3, 4, 6
Range: 5-10
Combination: 3, 4, 5-10, 8

Command Modes

VLT DOMAIN PROXY GW STATIC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>

Usage Information

You can configure the MAC address of a VLT peer in a remote VLT domain to associate with the static VLT proxy gateway and exclude a VLAN, or a range of VLANs, from proxy routing.

Example

```bash
Dell(conf)# vlt-domain 1
Dell(conf-vlt-domain)# proxy-gateway static
Dell(conf-vlt-domain-proxy-gw-static)# remote-mac-address 00:01:e8:06:95:ac
Dell(conf-vlt-domain-proxy-gw-static)# exclude-vlan 3
Dell(conf-vlt-domain-proxy-gw-static)#
```

peer-domain-link port-channel exclude-vlan

Configure the VLT port channel, which is connected to the remote VLT domain, for the proxy gateway or configure the VLANs you want to exclude from VLT proxy gateway.

S3048-ON

Syntax

```bash
[no] peer-domain-link port-channel interface-identifier exclude-vlan vlan-range
```

Parameters

- **port-channel**: Configure the proxy-gateway interface port-channel.
- **interface-identifier**: Enter the interface type.
- **vlan-range**: Enter the VLAN IDs that you want to exclude from the proxy gateway. The value can be a single VLAN ID, comma-separated VLAN IDs, a range of VLAN IDs, or a combination. For example:

  Comma-separated: 3, 4, 6
Range: 5-10

Combination: 3, 4, 5-10, 8

**Command Modes**

**VLT DOMAIN PROXY GW LLDP**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.1(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

You must configure the VLT port channel interface which is connecting to the remote VLT domain as peer-domain-link. You can also configure the VLANs you want to exclude from the VLT proxy gateway.

**Example**

```
Dell(conf)#vlt-domain 1
Dell(conf-vlt-domain)#proxy-gateway lldp
Dell(conf-vlt-domain-proxy-gw-lldp)#peer-domain-link port-channel 20 exclude-vlan 3
```

### proxy-gateway peer-timeout

Enables the VLT node to timeout the transmission of the peer MAC address when the VLT peer is down.

**S3048-ON**

**Syntax**

```
[no] peer-timeout value
```

**Parameters**

- **value**
  
  Enter the timeout value (in seconds). The range is from 1 to 65535. The default is `infinity`.

**Default**

Infinity

**Command Modes**

**VLT DOMAIN PROXY GW LLDP**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Removed the default value on the S-Series and Z-Series.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.</td>
</tr>
</tbody>
</table>

**Usage Information**

When a VLT peer goes down, the local VLT node stops sending its peer’s MAC address. If you configure this timeout, the local VLT node sends its peer’s MAC address until the timer expires.

Use this timer when you enable `vlt-peer-mac transmit`. A typical use example is a square VLT topology with a single link connecting to the remote peers.

**Example**

```bash
Dell(conf-vlt-domain-proxy-gw-lldp)# peer-timeout 5
```

### vlt-peer-mac transmit

Enables the device to transmit the peer MAC address along with its own MAC address in LLDP TLV packets to the remote VLT domain.

**S3048-ON**

**Syntax**

```bash
[no] vlt-peer-mac transmit
```

**Command Modes**

VLT DOMAIN PROXY GW LLDP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S4810, S4820T, S6000, and Z9000.</td>
</tr>
</tbody>
</table>

**Usage Information**

This command enables the device to transmit its VLT peer MAC address along with its own MAC address to the remote VLT domain. By default, a node sends only its own MAC address to the remote VLT domain.

This configuration is applicable only for an LLDP proxy gateway. A typical use example is a square VLT topology with single link connecting to the remote peers.

**Example**

```bash
Dell(conf-vlt-domain-proxy-gw-lldp)# vlt-peer-mac transmit
```
show vlt-proxy-gateway

Displays the VLT proxy gateway configuration.

S3048–ON

Syntax
show vlt-proxy-gateway [info] {lldp | static}

Parameters
lldp
Enter the keyword lldp to display details about the LLDP VLT proxy gateway configuration.

static
Enter the keyword static to display details about the static VLT proxy gateway configuration.

Command Modes
• EXEC
• EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.4(0.0) Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information
The proxy-gateway feature may go operationally down for any of the following reasons:

• LLDP is globally disabled.
• LDP is disabled per port.
• VLT port-channel is down.
• LLDP neighbor is down.

If any of these conditions is true, the proxy-gateway feature could be operationally down. If so, it is shown in the show command output.

When more than one VLT port-channel terminates on the same ToR, the show VLT proxy-gateway info lldp command output may show the port-channel ID incorrectly.

Example
Dell#show vlt proxy-gateway
VLT Proxy Gateway Brief
-------------------------
Config Mode: LLDP
Global LLDP Config Status: Enabled
peer-mac-transmit Status: Disabled

Dell#show vlt proxy-gateway info static
<table>
<thead>
<tr>
<th>Mac Address</th>
<th>Exclude Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:e8:8a:e8:f7</td>
<td>3,7-8</td>
</tr>
<tr>
<td>00:01:e8:8b:1c:c0</td>
<td>3,7-8</td>
</tr>
</tbody>
</table>

Dell#show vlt proxy-gateway info lldp
LagId Mac Address     Exclude Vlan
----- -----------     ------------
Po 55 00:01:e8:8a:e8:f7 3,7-8 << Macs learnt via port-channel 55
Po 55 00:01:e8:8b:1c:c0 3,7-8
Virtual Link Trunking (VLT)

Virtual link trunking (VLT) allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology.

VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

**NOTE:** When you launch the VLT link, the VLT peer-ship is not established if any of the following is TRUE:

- The VLT System-MAC configured on both the VLT peers do not match.
- The VLT Unit-Id configured on both the VLT peers are identical.
- The VLT System-MAC or Unit-Id is configured only on one of the VLT peers.
- The VLT domain ID is not the same on both peers.

If the VLT peer-ship is already established, changing the System-MAC or Unit-Id does not cause VLT peer-ship to go down.

Also, if the VLT peer-ship is already established and the VLT Unit-Id or System-MAC are configured on both peers, then changing the CLI configurations on the VLT Unit-Id or System-MAC is rejected if any of the following become TRUE:

- After making the CLI configuration change, the VLT Unit-Id becomes identical on both peers.
- After making the CLI configuration change, the VLT System-MAC do not match on both peers.

When the VLT peer-ship is already established, you can remove the VLT Unit-Id or System-MAC configuration from either or both peers. However, removing configuration settings can cause the VLT ports to go down if you configure the Unit-Id or System-MAC on only one of the VLT peers.

Topics:

- back-up destination
- clear vlt statistics
- delay-restore
- delay-restore abort-threshold
- lacp ungroup member-independent
- multicast peer-routing timeout
- peer-link port-channel
- peer-routing
- peer-routing-timeout
- primary-priority
- show vlt brief
- show vlt backup-link
- show vlt counters
- show vlt detail
- show vlt inconsistency
- show vlt mismatch
- show vlt role
- show vlt statistics
back-up destination

Configure the IPv4 or IPv6 address of the management interface on the remote VLT peer used as the VLT backup link endpoint for sending out-of-band (OOB) hello messages.

Syntax

```
back-up destination {ipv4-address | [ipv6 ipv6-address] [interval seconds]}
```

Parameters

- `ipv4-address`: Enter the IPv4 address of the backup destination.
- `ipv6`: Enter the keyword `ipv6` then an IPv6 address in the `X::X::X::X` format.
- `interval seconds`: Enter the keyword `interval` to specify the time interval to send hello messages. The range is from 1 to 5 seconds. The default is 1 second.

Defaults

1 second

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2) Added support for IPv6.
9.0.2.0 Introduced on the S6000.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.8.0 Introduced on the S4810.

clear vlt statistics

Clear the VLT operation statistics.

Syntax

```
clear vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]
```

1572  |  Virtual Link Trunking (VLT)
Parameters

- **domain**
  Clear the VLT statistics for the domain.
- **multicast**
  Clear the VLT statistics for multicast.
- **mac**
  Clear the VLT statistics for the MAC address.
- **arp**
  Clear the VLT statistics for ARP.
- **igmp-snoop**
  Clear the VLT statistics for IGMP snooping.
- **ndp**
  Clear the VLT statistics for NDP.

Command Modes

- EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Added multicast and ndp parameters.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Example

```
VLT ARP Statistics
----------------
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:19
ARP Reg Request rcvd:10
```

Related Commands

- `show vlt statistics` — displays statistics on VLT operations.

**delay-restore**

Configure the delay in bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.

**Syntax**

`delay-restore`
Parameters

delay-restore

Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLTI device reloads or after the peer-link restores between VLT peer switches. The range from 1 to 1200. The default is 90 seconds.

Defaults

Not configured.

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description

9.10(0.0) Introduced on the S6100–ON.

9.8(1.0) Introduced on the Z9100–ON.

9.8(0.0P5) Introduced on the S4048-ON.

9.8(0.0P2) Introduced on the S3048-ON.

9.7(0.0) Introduced on the S6000-ON.

9.5(0.1) Introduced on the Z9500.

9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

9.0.2.0 Introduced on the S6000.

9.0.0.0 Introduced on the Z9000.

8.3.19.0 Introduced on the S8420T.

8.3.12.0 Introduced on the S4810.

Usage Information

To delay the system from bringing up the VLT port for a brief period to allow IGMP snooping and Layer 3 routing protocols to converge, use the delay-restore command. Use this command:

- after a VLT device reloads.
- if the peer VLT device was up at the time the VLTI link failed.

Related Commands

- show vlt statistics — displays statistics on VLT operations.

**delay-restore abort-threshold**

Increase the boot up timer to a value greater than 60 seconds.

Syntax

delay-restore abort-threshold <interval>

To remove the boot up timer value, use the no delay-restore abort-threshold command.

Parameters

interval

Enter the interval value (in seconds) for the delay restore timer to abort. The range is from 1 to 1800 seconds. The default is 60 seconds.

This delay restore timer applies only during reload/boot-up and not in other scenarios (for example, during ICL flap).
Defaults

60 seconds

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S4820T, S4810, S6000, S5000, Z9000, S6000–ON and Z9500.</td>
</tr>
</tbody>
</table>

Usage Information

To abort the VLT delay restore timer value as the maximum threshold, during reload, apply the maximum time interval to the hold-down ICL peer-up in the start-up configurations.

**lacp ungroup member-independent**

Prevent possible loop during the VLT peer switch bootup or on a device that accesses the VLT domain.

**Syntax**

```plaintext
lacp ungroup member-independent {vlt | port-channel}
```

**Parameters**

- `vlt` Force all VLT LACP members to become switchports.
- `port-channel` Force all LACP port-channel members to become switchports.

**Defaults**

Not configured.

**Command Modes**

CONFIGURATION

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(12.0)</td>
<td>Added port-channel parameter on the S4810.</td>
</tr>
</tbody>
</table>
LACP on the VLT ports (on a VLT switch or access device), which are members of the VLT, are not brought up until the VLT domain is recognized on the access device.

During boot-up in a stacking configuration, the system must be able to reach the DHCP server with the boot image and configuration image. To receive an offer on static LAGs between switches, only untagged DHCP requests are sent to the DHCP server. Configure the DHCP server to start in BMP mode.

If the switches are connected using LACP port-channels (for example, the VLT peer and top of rack [ToR]), use the port-channel option on the ToR-side configuration to allow member ports of an ungrouped LACP port-channel to inherit VLAN membership of that port channel. This ensures untagged VLT peer device packets reach the DHCP server on the ToR.

To ungroup the VLT and port-channel configurations, use the `no lacp ungroup member independent` command on a VLT port channel.

```
Example
Dell(conf)#lacp ungroup member-independent ?
port-channel LACP port-channel members become switchports
vlt All VLT LACP members become switchports
```

To retain synced multicast routes or synced multicast outgoing interface (OIF) after a VLT peer node failure, configure the timeout value for a VLT node.

```
multicast peer-routing timeout value
```

To restore the default value, use the `no multicast peer-routing timeout` command.

```
Parameters
value Enter the timeout value (in seconds). The range is from 1 to 1200. The default is 150.
```

```
Command Modes
VLT DOMAIN (conf-vlt-domain)
```

```
Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
```

```
Version Description
9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.2(0.0) Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2) Introduced on the Z9000, S4810, and S4820T.
```
peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

Syntax
peer-link port-channel port-channel-number {peer-down-vlan vlan id}

Parameters
- **port-channel-number**: Enter the port-channel number that acts as the interconnect trunk. The range is from 1 to 128.
- **peer-down-vlan vlan id**: Enter the keywords peer-down-vlan then a VLAN ID to configure the VLAN that the VLT peer link uses when the VLT peer is down.

Defaults
Not configured.

Command Modes
VLT DOMAIN

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Added support for the peer-down-vlan option.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information
To configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down, use the peer-down-vlan option. When a VLT peer with bare metal provisioning (BMP) is booting up, it sends untagged DHCP discover packets to its peer over the VLTi. To ensure that the DHCP discover packets are forwarded to the VLAN that has the DHCP server, use this configuration.

peer-routing

Enable Layer 3 (L3) VLT peer-routing. This command is applicable for both IPv6 and IPv4 interfaces.

Syntax
peer-routing
To disable L3 VLT peer-routing, use the `no peer-routing` command.

**Defaults**

Disabled.

**Command Modes**

VLT DOMAIN (conf-vlt-domain)

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added the support for IPV6 / IPV4.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

**peer-routing-timeout**

Configure the delay after which peer routing disables when the peer is unavailable. This command is applicable for both IPv6 and 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 infinity.

**Command Modes**

VLT DOMAIN (conf-vlt-domain)

**Default**

Infinity

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for default value on the S-Series and Z-Series.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>
Version | Description
---|---
9.4(0.0) | Added the support for IPV6 / IPV4.
9.2(0.2) | Introduced on the Z9000, S4810, and S4820T.
9.0.2.0 | Introduced on the S6000.

Usage Information | When the timer expires, the software checks to see if the VLT peer is available. If the VLT peer is not available, peer-routing disables on that peer.
If you do not configure this delay value, peer-routing is not disabled even when the peer is unavailable.

**primary-priority**

Assign the priority for master election among VLT peers.

**Syntax**
```
[no] primary-priority
```

**Parameters**
- `value`  
  
  To configure the primary role on a VLT peer, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535. The default value is **32768**.

**Default**

**Command Modes**

- **VLT DOMAIN**

**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.
9.8(1.0) | Introduced on the Z9100-ON.
9.8(0.0P5) | Introduced on the S4048-ON.
9.8(0.0P2) | Introduced on the S3048-ON.
9.7(0.0) | Introduced on the S6000-ON.
9.5(0.1) | Introduced on the Z9500.
9.2(0.0) | Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0 |Introduced on the S6000.
8.3.19.0 | Introduced on the S4820T.
8.3.8.0 | Introduced on the S4810.

**Usage Information**

After you configure a VLT domain on each peer switch and connect (cable) the two VLT peers on each side of the VLT interconnect, the system elects a primary and secondary VLT peer device. To configure the primary and secondary roles before the election process, use the primary-priority command. Enter a lower value on the primary peer and a higher value on the secondary peer.

If the primary peer fails, the secondary peer (with the higher priority) takes the primary role. If the primary peer (with the lower priority) later comes back online, it is assigned the secondary role (there is no preemption).
show vlt brief

Displays summarized status information about VLT domains configured on the switch.

Syntax
show vlt brief

Default
Not configured.

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(8.0)</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information
The version shown in the show vlt brief output command displays the VLT version number which is different from the Dell Networking OS version number. VLT version numbers begin with odd numbers.

Example (Brief)
Dell#show vlt brief
VLT Domain Brief
------------------
Domain ID                     : 1
Role                          : Secondary
Role Priority                 : 32768
ICL Link Status               : Up
HeartBeat Status              : Up
VLT Peer Status               : Up
Version                       : 6(3)
Local System MAC address      : 00:01:e8:8a:e9:91
Remote System MAC address     : 00:01:e8:8a:e9:76
Remote system version         : 6(3)
Delay-Restore timer           : 90 seconds
Delay-Restore Abort Threshold : 60 seconds
Peer-Routing                  : Disabled
Peer-Routing-Timeout timer    : 0 seconds
Multicast peer-routing timeout: 150 seconds
Dell#

show vlt backup-link

Displays information about the backup link operation.

Syntax
show vlt backup-link
show vlt counters

Displays counter information.

Syntax

show vlt counters [arp | igmp-snoop | interface | mac | ndp]

Parameters

arp
Enter the keyword arp to display the ARP counter information for the VLT.

igmp-snoop
Enter the keywords igmp-snoop to display the igmp-snooping counter information for the VLT.

interface
Enter the keyword interface to display the interface counter information for the VLT.

mac
Enter the keyword mac to display the MAC address counter information for the VLT.

ndp
Enter the keyword ndp to display the VLT counter information for NDP.

Default
Not configured.

Command Modes
EXEC
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Usage Information

If you do not add a parameter such as arp or mac, the output displays all the counters.

Example

```
Dell# show vlt counter
Total VLT counters
-------------------------
L2 Total MAC-Address Count :
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
ARP entries count :
```

Example (igmp-snoop)

```
Dell# show vlt counter igmp-snoop
Total IGMP VLT counters
----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count : 5
```

Example (igmp-snoop interface port-channel)

```
Dell# show vlt counter igmp-snoop interface port-channel 2
VLT Port-ID: 2 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 0
IGMP Mcast Groups count : 5
```

```
Dell# show vlt counter igmp-snoop interface port-channel 100
VLT Port-ID: 100 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count : 0
```

Example (NDP and Non-VLT ARP)

```
Dell# show vlt counters
Total VLT Counters
-------------------
L2 Total MAC-Address Count : 2
Total Arp Entries Learnt : 0
Total Arp Entries Synced : 0
Total Non-VLT Arp entries Learnt : 0
Total Non-VLT Arp Entries Synced : 0
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
Total VLT Ndp Entries Learnt : 2
Total VLT Ndp Entries Synced : 0
```
show vlt detail

Displays detailed status information about VLT domains configured on the switch.

Syntax       show vlt detail

Default      Not configured.

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

Example

```
Dell# Dell(conf-if-vl-100)#show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
---------- ----------- ------------ ----------- -------------
 10          10          UP           UP         100, 200, 300, 400,
```

show vlt inconsistency

Display run-time inconsistencies in the incoming interface (IIF) for spanned multicast routes (mroutes).

Syntax       show vlt inconsistency ip mroute

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
**show vlt mismatch**

Display mismatches in VLT parameters.

**Syntax**

```
show vlt mismatch
```

**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced support for Q-in-Q implementation over VLT on the S-Series and Z-Series. Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell#show vlt mismatch
Domain
--------
Parameters    Local     Peer
----------    -----     -----  
Unit-ID       1          2
Vlan-config
----------
Vlan-ID    Local Mode  Peer Mode
```
Example for Q-in-Q implementation over VLT:

```
Dell#show vlt mismatch
Domain
------
Parameters      Local      Peer
--------        -----      ----
PB for stp      Enabled    Disabled

Vlan-type-config
----------------
Codes:: P - Primary, C - Community, I - Isolated, N - Normal vlan, M - Vlan-stack

Vlan-ID      Local    Peer
--------      -----    ----
100          N        M

Port-type-config
----------------
Codes:: p - PVLAN Promiscuous port, h - PVLAN Host port, t - PVLAN Trunk port,
        mt - Vlan-stack trunk port, mu - Vlan-stack access port, n - Normal port

Vlt Lag      Local    Peer
--------      -----    ----
128          mt        mu

Vlan-stack protocol-type
------------------------
Local      Peer
-----      ----
0x4100      0x8100

VLT-VLAN config
---------------
Local Lag  Peer Lag Local VLANs Peer VLANs
--------  -------- ----------- ----------
128       128       4094          100

Dell#
```
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### Example

```
Dell_VLTpeer1# show vlt role

VLT Role
-------
VLT Role: Primary
System MAC address: 00:01:e8:8a:df:bc
System Role Priority: 32768
Local System MAC address: 00:01:e8:8a:df:bc
Local System Role Priority: 32768

Dell_VLTpeer2# show vlt role

VLT Role
-------
VLT Role: Secondary
System MAC address: 00:01:e8:8a:df:bc
System Role Priority: 32768
Local System MAC address: 00:01:e8:8a:df:e6
Local System Role Priority: 32768
```

### show vlt statistics

Displays VLT operations statistics.

**Syntax**

```
show vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]
```

**Parameters**

- **arp**
  - Enter the keyword `arp` to display the ARP VLT statistics.
- **domain**
  - Enter the keyword `domain` to display the domain VLT statistics.
- **igmp-snoop**
  - Enter the keywords `igmp-snoop` to display the IGMP snooping VLT statistics.
- **mac**
  - Enter the keyword `mac` to display the VLT MAC addresses VLT statistics.
- **multicast**
  - Enter the keyword `multicast` to display the multicast VLT statistics.
- **ndp**
  - Enter the keyword `ndp` to display the NDP VLT statistics.

**Default**

Not configured.
**Command Modes**

EXEC

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.2)</td>
<td>Added parameters multicast and ndp</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.12.0</td>
<td>Added support in the output for ARP, MAC, and IGMP snooping.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Related Commands**

- `clear vlt statistics` — clears the statistics on VLT operations.

**Example**

```bash
NOTE: The following example shows the statistics for all the VLT parameters. If you enter a specific keyword, such as `mac`, only the statistics for that VLT parameter displays.

Dell_VLTpeer1# show vlt statistics
VLT Statistics
----------------
HeartBeat Messages Sent: 930
HeartBeat Messages Received: 909
ICL Hello's Sent: 927
ICL Hello's Received: 910
Domain Mismatch Errors: 0
Version Mismatch Errors: 0
Config Mismatch Errors: 0

VLT MAC Statistics
-------------------
L2 Info Pkts sent:6, L2 Mac-sync Pkts Sent:0
L2 Info Pkts Rcvd:3, L2 Mac-sync Pkts Rcvd:2
L2 Reg Request sent:1
L2 Reg Request rcdv:2
L2 Reg Response sent:1
L2 Reg Response rcdv:1

VLT Igmp-Snooping Statistics
-------------------------------
IGMP Info Pkts sent: 4
IGMP Info Pkts Rcvd: 1
IGMP Reg Request sent: 1
IGMP Reg Request rcdv: 2
IGMP Reg Response sent: 1
IGMP Reg Response rcdv: 1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcdv: 10
IGMP Tunnel PDUs sent: 10
IGMP Tunnel PDUs rcdv: 19
```
show vlt statistics igmp-snoop

Displays the informational packets and IGMP control PDUs that are exchanged between VLT peer nodes.

Syntax
show vlt statistics igmp-snoop

Default
Not configured.

Command Modes
EXEC

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.12.0 Introduced on the S4810.

Example
Dell_VLTpeer1#show vlt statistics igmp-snoop
VLT Igmp-Snooping Statistics
----------------------------------
IGMP Info Pkts sent: 4
IGMP Info Pkts Rcvd: 1
IGMP Reg Request sent: 1
IGMP Reg Request rcvd: 2
IGMP Reg Response sent: 1
IGMP Reg Response rcvd: 1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcvd: 10
 IGMP Tunnel PDUs sent: 10
 IGMP Tunnel PDUs rcvd: 19

**system-mac**

Reconfigure the default MAC address for the domain.

**Syntax**

```plaintext
system-mac mac-address
```

**Parameters**

- `mac-address` Enter the system MAC address for the VLT domain.

**Defaults**

Not configured.

**Command Modes**

VLT DOMAIN

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

**Usage Information**

When you create a VLT domain on a switch, the Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations.

To reconfigure the default MAC address for the domain, use the `system-mac` command. The MAC address must be in the `nn:nn:nn:nn:nn:nn` format. Also reconfigure the same MAC address on the VLT peer switch.

**unit-id**

Configure the default unit ID of a VLT peer switch.

**Syntax**

```plaintext
unit-id [0 | 1]
```

**Parameters**

- `0 | 1` Configure the default unit ID of a VLT peer switch. Enter `0` for the first peer. 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
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### Usage Information

When you create a VLT domain on a switch, the 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. To explicitly configure the unit ID of a VLT peer, use the unit-id command. Configure a different unit ID (0 or 1) on each peer switch.

This command minimizes the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots.

**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**

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
</tbody>
</table>
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 generates and VLT does not launch.

Related Commands
- `show vlt brief` — display the delay-restore value.

vlt-peer-lag port-channel
Associate the port channel to the corresponding VLT peer port channel for the VLT connection to an attached device.

Syntax
```plaintext
vlt-peer-lag port-channel id-number
```

Parameters
- `id-number` Enter the respective VLT port-channel number of the peer device. The range is from 1 to 128.

Defaults
Not configured.

Command Modes
INTERFACE PORT-CHANNEL

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>9.2(0.0)</td>
<td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td>
</tr>
</tbody>
</table>

show vlt private-vlan
Display the private VLAN (PVLAN) associated with the VLT LAG for VLT peer nodes.

Syntax
```plaintext
show vlt private-vlan
```

Command Modes
EXEC
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.1)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.3(0.0)</td>
<td>Introduced on the Z9000, S4810, and S4820T.</td>
</tr>
</tbody>
</table>

### 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. The ICL Status field displays the type of 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

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>ICL Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td>V (*)</td>
</tr>
<tr>
<td>20 (C)</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>30 (I)</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>T</td>
</tr>
<tr>
<td>50 (C)</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>60 (I)</td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>
Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking OS.

Topics:
- IPv4 VRRP Commands
- IPv6 VRRP Commands

IPv4 VRRP Commands

The following are IPv4 VRRP commands.

advertise-interval

Set the time interval between VRRP advertisements.

Syntax

advertise-interval {seconds | centisecs centisecs }

To return to the default settings, use the no advertise-interval command.

Parameters

seconds

Enter the number of seconds. The range is from 1 to 255. The default is 1 second.

centisecs centisecs

Enter the keyword centisecs then the number of centisecs in multiples of 25 centisecs. The range is 25 to 4075 centisecs in multiples of 25 centisecs.

Defaults

1 second or 100 centisecs.

Command Modes

INTERFACE-VRRP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**
Dell Networking recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, change it on all routers.

### authentication-type

Enable authentication of VRRP data exchanges.

**Syntax**

```
authentication-type simple [encryption-type] password
```

To delete an authentication type and password, use the `no authentication-type` command.

**Parameters**

- **simple**
  - Enter the keyword `simple` to specify simple authentication.
- **encryption-type**
  - Enter one of the following:
    - `0` (zero) specifies an unencrypted authentication data follows.
    - `7` (seven) specifies a hidden authentication data follows.
    - `LINE` is the unencrypted (cleartext) authentication data.
- **password**
  - Enter a character string up to eight characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

**Defaults**

Not configured.

**Command Modes**

VRRP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>
**clear counters vrrp**

Clear the counters maintained on VRRP operations.

**Syntax**

```
clear counters vrrp [vrrp-id] [ipv6]
```

**Parameters**

- `vrrp-id`  
  (OPTIONAL) Enter the number of the VRRP group ID to clear the group's counters. The range is from 1 to 255.

- `ipv6`  
  (OPTIONAL) Enter the keyword `ipv6` to clear counters from the IPv6 VRRP group.

**Command Modes**

EXEC Privilege

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Added support to clear the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3(19.0)</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3(11.1)</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3(7.0)</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
Usage Information

**NOTE:** This command also enables you to clear the port configurations 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 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`.
- For ON platforms, you can specify multiple ports as `slot/port/0 - slot/port/4`. 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 1/1/1 - 1/1/4`.

**debug vrrp**

Enable VRRP debugging.

**Syntax**

```
debug vrrp [vrrp-id] {all | bfd | database | interface | ipv6 | packets | state | timer}
```

To disable debugging, use the `no debug vrrp [vrrp-id] {all | bfd | database | interface | ipv6 | packets | state | timer}` command.

**Parameters**

- **vrrp-id** (OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
- **all** Enter the keyword `all` to enable debugging of all VRRP groups.
- **bfd** Enter the keyword `bfd` to enable debugging of VRRP BFD interactions.
- **database** Enter the keyword `database` to enable debugging of configuration changes.
- **interface** Enter the following keywords and the interface information:
  - For Port Channel interface types, enter the keywords `port-channel` then the number.
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
- **interface** Enter the keyword `interface` to enable debugging of interface state changes.
- **ipv6** Enter the keyword `ipv6` to enable debugging for IPv6.
- **packets** Enter the keyword `packets` to enable debugging of VRRP control packets.
- **state** Enter the keyword `state` to enable debugging of VRRP state changes.
- **timer** Enter the keyword `timer` to enable debugging of the VRRP timer.

**Command Modes** EXEC Privilege

**Command History** This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.
**description**

Configure a short text string describing the VRRP group.

```
Syntax

description text

To delete a VRRP group description, use the no description command.
```

**Parameters**

- **text**
  
Enter a text string up to 80 characters long.

**Defaults**

Not enabled.

**Command Modes**

VRRP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If you do not specify an option, debug is active on all interfaces and all VRRP groups.
disable

Disable a VRRP group.

Syntax
disable

To re-enable a disabled VRRP group, use the no disable command.

Command Modes
VRRP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100–ON.
9.8(1.0) Introduced on the Z9100–ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.2(1.0) Introduced on the Z9500.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Usage Information
To enable VRRP traffic, assign an IP address to the VRRP group using the virtual-address command and enter no disable.

Related Commands
• virtual-address — specify the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

Syntax
hold-time {seconds | centisecs centisecs}
To return to the default value, use the `no hold-time` command.

**Parameters**

- **seconds**
  - Enter the number of seconds. The range is from 0 to 65535. The default is **zero (0) seconds**.

- **centisecs**
  - Enter the keyword `centisecs` then the number of `centisecs` in units of 25 centisecs. The range is from 0 to 65525 in units of 25 centisecs.

**Defaults**

- **zero (0) seconds or (0) centiseconds**

**Command Modes**

- VRRP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P6)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.5(0.0)</td>
<td>Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

If a switch is a MASTER and you change the hold timer, disable and re-enable VRRP for the new hold timer value to take effect.

**Related Commands**

- `disable` — disables a VRRP group.

### preempt

To preempt or become the MASTER router, configure a BACKUP router with a higher priority value.

**Syntax**

`preempt`

To prohibit preemption, use the `no preempt` command.

**Defaults**

- Enabled (that is, a BACKUP router can preempt the MASTER router).

**Command Modes**

- VRRP
priority

Specify a VRRP priority value for the VRRP group. The VRRP protocol uses this value during the MASTER election process.

**Syntax**

```
priority priority
```

To return to the default value, use the no priority command.

**Parameters**

- `priority` Enter a number as the priority. Enter 255 only if the router’s virtual address is the same as the interface’s primary IP address (that is, the router is the OWNER). The range is from 1 to 255. The default is 100.

**Defaults**

100

**Command Modes**

VRRP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>
show config

View the non-default VRRP configuration.

Syntax

```
show config [verbose]
```

Parameters

- **verbose** (OPTIONAL) Enter the keyword `verbose` to view all the VRRP group configuration information, including default information.

Command Modes

VRRP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group’s virtual address with same IP address as the interface’s primary IP address and change the priority of the VRRP group to 255.

If you set the `priority` command to 255 and the `virtual-address` is not equal to the interface’s primary IP address, an error message appears.
show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the Dell Networking OS returns No Active VRRP group.

Syntax

```
show vrrp [vrrp-id][brief][interface type][ipv6][interface type][vrf vrf-name]
```

Parameters

- **vrrp-id** (OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.
- **brief** (OPTIONAL) Enter the keyword brief to view a table of information about the VRRP groups.
- **interface type** (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a VLAN interface, enter the keyword vlan, and then the VLAN ID. The VLAN ID range is from 1 to 4094.
- **ipv6** (OPTIONAL) Enter the keyword ipv6 to view only VRRP IPv6 groups.
- **vrf vrf-name** (OPTIONAL) Enter the keyword vrf and then the name of the VRF to view active VRRP groups corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.4.(0.0)</td>
<td>Added support for VRF.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.11.1</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.7.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series.</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**

The following describes the `show vrrp brief` command.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Lists the interface type, slot, and port of the configured VRRP group.</td>
</tr>
<tr>
<td>Grp</td>
<td>Displays the VRRP group ID.</td>
</tr>
<tr>
<td>Pri</td>
<td>Displays the priority value assigned to the interface. If you configured the track command to track that interface and you disable the interface, the cost is subtracted from the priority value assigned to the interface.</td>
</tr>
<tr>
<td>Pre</td>
<td>States whether preempt is enabled on the interface:</td>
</tr>
<tr>
<td></td>
<td>• Y = Preempt is enabled.</td>
</tr>
<tr>
<td></td>
<td>• N = Preempt is not enabled.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the operational state of the interface using one of the following:</td>
</tr>
<tr>
<td></td>
<td>• NA/IF (the interface is not available).</td>
</tr>
<tr>
<td></td>
<td>• MASTER (the interface associated with the MASTER router).</td>
</tr>
<tr>
<td></td>
<td>• BACKUP (the interface associated with the BACKUP router).</td>
</tr>
<tr>
<td>Master addr</td>
<td>Displays the IP address of the MASTER router.</td>
</tr>
<tr>
<td>Virtual addr(s)</td>
<td>Displays the virtual IP addresses of the VRRP routers associated with the interface.</td>
</tr>
</tbody>
</table>

**Example (Brief)**

```
Dell> Interface Grp Pri Pre State Master addr Virtual addr(s)
Description----------------------------------
Gi 1/37 1 100 Y Master 200.200.200.200 200.200.200.201
Description
Gi 1/37 3 100 Y Master 1.1.1.1 1.1.1.2
short desc
Dell>
```

**Usage Information**

The following describes the `show vrrp` command.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet 1/3...</td>
<td>Displays the interface, VRRP group ID, and network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.</td>
</tr>
<tr>
<td>State: master...</td>
<td>Displays the interface’s state:</td>
</tr>
<tr>
<td></td>
<td>• Na/If (not available)</td>
</tr>
<tr>
<td></td>
<td>• master (MASTER virtual router)</td>
</tr>
<tr>
<td></td>
<td>• backup (BACKUP virtual router)</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Also displays</td>
<td>displays the interface's priority and IP address of the MASTER.</td>
</tr>
<tr>
<td>Hold Down:...</td>
<td>Displays additional VRRP configuration information:</td>
</tr>
<tr>
<td></td>
<td>- Hold Down displays the hold down timer interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>- Preempt displays TRUE if preempt is configured and FALSE if preempt is</td>
</tr>
<tr>
<td></td>
<td>not configured.</td>
</tr>
<tr>
<td></td>
<td>- AdvInt displays the Advertise Interval in seconds.</td>
</tr>
<tr>
<td>Adv rcvd:...</td>
<td>Displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>- Adv rcvd displays the number of VRRP advertisements received on the</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>- Adv sent displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>- Gratuitous ARP sent displays the number of gratuitous ARPs sent.</td>
</tr>
<tr>
<td>Virtual MAC address</td>
<td>Displays the virtual MAC address of the VRRP group.</td>
</tr>
<tr>
<td>Virtual IP address</td>
<td>Displays the virtual IP address of the interface's VRRP router.</td>
</tr>
<tr>
<td>Authentication:....</td>
<td>States whether authentication is configured for the VRRP group. If it is</td>
</tr>
<tr>
<td></td>
<td>configured, this lists the authentication type and password.</td>
</tr>
<tr>
<td>Tracking states:...</td>
<td>Displays if the track command is configured on an interface. Also displays</td>
</tr>
<tr>
<td></td>
<td>the following information about the tracked interface:</td>
</tr>
<tr>
<td></td>
<td>- Dn or Up states whether the interface is down or up.</td>
</tr>
<tr>
<td></td>
<td>- The interface type slot/port information.</td>
</tr>
</tbody>
</table>

**Example**

```
Dell> show vrrp
------------------
GigabitEthernet 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 GigabitEthernet 1/17 priority-cost 10
------------------
GigabitEthernet 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 GigabitEthernet 2/1 priority-cost 10
  Up GigabitEthernet 1/17 priority-cost 10
Dell>
```
Example (VRRP VRF)

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

- **interface** (OPTIONAL) Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a VLAN interface, enter the keyword `vlan`, and then the VLAN ID. The VLAN ID range is from 1 to 4094.

- **priority-cost** (OPTIONAL) Enter a number as the amount to subtract from the priority value. The range is from 1 to 254. The default is `10`.

Defaults

```
priority cost = 10
```

Command Modes

- **VRRP**

Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>7.6.1.0</td>
<td>Introduced on the S-Series (S50 only).</td>
</tr>
<tr>
<td>7.5.1.0</td>
<td>Introduced on the C-Series.</td>
</tr>
<tr>
<td>6.2.1.1</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information

If you disable the interface, 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 virtual router IP addresses in the VRRP group. To start sending VRRP packets, set at least one virtual IP address for the VRRP group.

**Syntax**

```
virtual-address ip-address1 [... ip-address12]
```

To delete one or more virtual IP addresses, use the no virtual-address ip-address1 [... ip-address12] command.

**Parameters**

- `ip-address1` Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface’s primary IP address.
- `... ip-address12` (OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface’s primary IP address.

**Defaults**

Not configured.

**Command Modes**

VRRP

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

**Version**

- 9.8(0.0P5) Introduced on the S4048-ON.
- 9.8(0.0P2) Introduced on the S3048-ON.
- 9.7(0.0) Introduced on the S6000-ON.
- 9.0.2.0 Introduced on the S6000.
- 8.3.19.0 Introduced on the S4820T.
- 8.3.11.1 Introduced on the Z9000.
- 8.3.7.0 Introduced on the S4810.
- 7.6.1.0 Introduced on the S-Series.
- 7.5.1.0 Introduced on the C-Series.
- 7.4.1.0 Introduced support for telnetting to the VRRP group IP address assigned using this command.
- 6.2.1.1 Introduced on the E-Series.

**Usage Information**

The VRRP group only becomes active and sends VRRP packets when you configure a virtual IP address. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the virtual-address command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group’s virtual IP address with the same address as the interface’s primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual IP addresses configured in all VRRP groups.
vrrp delay minimum

Set the delay time for VRRP initialization after an interface comes up.

Syntax
vrrp delay minimum seconds

Parameters
seconds Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. The range is from 0 to 900 (0 indicates no delay).

Defaults
0

Command Modes INTERFACE

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.0.2.0 Introduced on the S6000.
9.0.0.0 Introduced on the Z9000.
8.3.19.0 Introduced on the S4820T.
8.3.8.0 Introduced on the S4810.

Usage Information
This command applies to a single interface. When you use this command with the vrrp delay reload command, the later timer rules VRRP enabling. For example, if vrrp delay reload is 600 and 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
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.0.2.0</td>
<td>Introduced on the S6000.</td>
</tr>
<tr>
<td>9.0.0.0</td>
<td>Introduced on the Z9000.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.8.0</td>
<td>Introduced on the S4810.</td>
</tr>
</tbody>
</table>

### Usage Information

This command applies to all the VRRP interfaces on a system. When you use this command with the `vrrp delay minimum` command, the later timer rules VRRP enabling. For example, if `vrrp delay reload` is 600 and `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.

For the delay timers to take effect, save the configuration and reload the system.

### Related Command
- `vrrp delay minimum` — sets the delay time for VRRP initialization after a line card reboot.

---

**vrrp-group**

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

### Syntax

```
vrrp-group vrrp-id
```

### Parameters

- **vrrp-id**
  - Enter a number as the group ID. The range is from 1 to 255.

### Defaults

Not configured.

### Command Modes

INTERFACE

### Command History

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
</tbody>
</table>
Version Description
9.7(0.0) Introduced on the S6000-ON.
9.0.2.0 Introduced on the S6000.
8.3.19.0 Introduced on the S4820T.
8.3.11.1 Introduced on the Z9000.
8.3.7.0 Introduced on the S4810.
7.6.1.0 Introduced on the S-Series.
7.5.1.0 Introduced on the C-Series.
6.2.1.1 Introduced on the E-Series.

Usage Information
The VRRP group only becomes active and sends VRRP packets when you configure a virtual IP address. When you delete the virtual IP address, the VRRP group stops sending VRRP packets.

Related Command
- `virtual-address` — assigns up to 12 virtual IP addresses per VRRP group.

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.

Parameters
- `2` Enter the keyword 2 to specify VRRP version 2 as defined by RFC 3768, Virtual Router Redundancy Protocol.
- `3` Enter the keyword 3 to specify VRRP version 3 as defined by RFC 5798, Virtual Router Redundancy Protocol.
- `both` Enter the keyword both for in-service migration from VRRP version 2 to VRRP version 3.

Defaults
2

Command Modes
VRRP

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

Version Description
9.10(0.0) Introduced on the S6100-ON.
9.8(1.0) Introduced on the Z9100-ON.
9.8(0.0P5) Introduced on the S4048-ON.
9.8(0.0P2) Introduced on the S3048-ON.
9.7(0.0) Introduced on the S6000-ON.
9.5(0.1) Introduced on the Z9500.
### IPv6 VRRP Commands

The following are IPv6 VRRP commands.

- clear counters vrrp ipv6
- debug vrrp ipv6
- show vrrp ipv6
- vrrp-ipv6-group

The following commands apply to IPv4 and IPv6:

- advertise-interval
- description
- disable
- hold-time
- preempt
- priority
- show config
- virtual-address

#### clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

**Syntax**

```
clear counters vrrp ipv6 [vrid | vrf vrf-name]
```

**Parameters**

- `vrid`  
  (OPTIONAL) Enter the number of an IPv6 VRRP group; range is from 1 to 255.

- `vrf vrf-name`  
  (OPTIONAL) Enter the name of a VRF instance to clear the counters of all IPv6 VRRP groups in the specified VRF. The maximum is 32 characters.

**Command Modes**

EXEC Privilege
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

### Command History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.9(0.0)</td>
<td>Added support to clear the interface configurations corresponding to a range of ports.</td>
</tr>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series, C-Series, and S-Series. Support was added for IPv6 VRRP groups in nondefault VRF instances.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

### Usage Information

- **NOTE:** You can also clear the port configurations corresponding to a range of ports. For Open Networking (ON) platforms, the notation for specifying the port range in the command is different from how you specify the port range in non-ON platforms.

  - For non-ON platforms, 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`.
  - For ON platforms, you can specify multiple ports as `slot/port/[subport] - slot/port/[subport]`. 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 1/1/1 - 1/1/4`.

---

**debug vrrp ipv6**

Enable VRRP debugging.

**Syntax**

```
debug vrrp ipv6 interface [vrid] {all | packets | state | timer}
```

**Parameters**

- `interface` Enter the following keywords and the interface information:
  - For a 1-GigabitEthernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
  - For a Port Channel interface, enter the keywords `port-channel`, and then a number.
  - For a VLAN interface, enter the keyword `vlan`, and then the VLAN ID. The VLAN ID range is from 1 to 4094.

- `vrid` (OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.

- `all` Enter the keyword `all` to enable debugging of all VRRP groups.
<table>
<thead>
<tr>
<th>bfd</th>
<th>Enter the keyword bfd to enable debugging of all VFFP BFD interactions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>database</td>
<td>Enter the keyword database to display changes related to group, prefix, and interface entries in the VRRP table.</td>
</tr>
<tr>
<td>packets</td>
<td>Enter the keyword packets to enable debugging of VRRP control packets.</td>
</tr>
<tr>
<td>state</td>
<td>Enter the keyword state to enable debugging of VRRP state changes.</td>
</tr>
<tr>
<td>timer</td>
<td>Enter the keyword timer to enable debugging of the VRRP timer.</td>
</tr>
</tbody>
</table>

**Command Modes**  
EXEC Privilege

**Command History**  
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100–ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100–ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.4.1.0</td>
<td>Introduced on E-Series, C-Series, and S-Series. Support was added for IPv6 VRRP groups in nondefault VRF instances.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

**Usage Information**  
If you do not specify an option, debugging is active on all interfaces and all VRRP groups.

### show vrrp ipv6

View the active IPv6 VRRP groups. If no VRRP groups are active, the Dell Networking OS returns No Active VRRP group.

**Syntax**  
show vrrp ipv6 [vrid] [interface] [brief] [vrf vrf-name]

**Parameters**

- **vrid**  
  (OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.

- **interface**  
  Enter the following keywords and the number information:
  - For a 1-GigabitEthernet interface, enter the keyword GigabitEthernet then the slot/port information.
  - For a 10-Gigabit Ethernet interface, enter the keyword TenGigabitEthernet then the slot/port information.
  - For a port channel interface, enter the keywords port-channel, and then a number.
  - For a VLAN interface, enter the keyword vlan, and then a number from 1 to 4094.
brief (OPTIONAL) Enter the keyword brief to view a table of information on the VRRP groups.

vrf vrf-name Enter the keyword vrf then the name of the VRF to view IPv6 VRRP groups corresponding to that VRF.

Command Modes
- EXEC
- EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.3.19.0</td>
<td>Introduced on the S4820T.</td>
</tr>
<tr>
<td>8.3.10.0</td>
<td>Introduced on the S4810.</td>
</tr>
<tr>
<td>8.3.2.0</td>
<td>Introduced on the E-Series.</td>
</tr>
</tbody>
</table>

Usage Information
The following describes the show vrrp ipv6 command.

<table>
<thead>
<tr>
<th>Line starting with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet...</td>
<td>Displays the interface, VRRP group ID, and network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network IP address.</td>
</tr>
<tr>
<td>VRF</td>
<td>VRF instance to which the VRRP group interface belongs.</td>
</tr>
<tr>
<td>State: master...</td>
<td>Displays the interface’s state:</td>
</tr>
<tr>
<td></td>
<td>• Na/If (not available)</td>
</tr>
<tr>
<td></td>
<td>• master (MASTER virtual router)</td>
</tr>
<tr>
<td></td>
<td>• backup (BACKUP virtual router)</td>
</tr>
<tr>
<td></td>
<td>Also displays the interface’s priority and IP address of the MASTER.</td>
</tr>
<tr>
<td>Hold Down:...</td>
<td>Displays additional VRRP configuration information:</td>
</tr>
<tr>
<td></td>
<td>• Hold Down displays the hold down timer interval in seconds.</td>
</tr>
<tr>
<td></td>
<td>• Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured.</td>
</tr>
<tr>
<td></td>
<td>• AdvInt displays the Advertise Interval in seconds.</td>
</tr>
<tr>
<td>Adv rcvd:...</td>
<td>Displays counters for the following:</td>
</tr>
<tr>
<td></td>
<td>• Adv rcvd displays the number of VRRP advertisements received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Adv sent displays the number of VRRP advertisements sent on the interface.</td>
</tr>
<tr>
<td></td>
<td>• Bad pkts rcvd displays the number of invalid packets received on the interface.</td>
</tr>
</tbody>
</table>
Line starting with | Description
---|---
Virtual MAC address | Displays the virtual MAC address of the VRRP group.
Virtual IP address | Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states... | Displays information on the tracked interfaces or objects configured for a VRRP group (track command), including:
  - UP or DOWN state of the tracked interface or object (Up or Dn).
  - Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object.
  - Cost subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.

Example

```
Dell# show vrrp ipv6
------------------
  State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9 (local)
  Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
  Accept Mode: FALSE, Master AdvInt: 100 centisec
  Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
  Virtual MAC address: 00:00:5e:00:02:ff
  Virtual IP address: 1::255 fe80::255
```

**vrrp-ipv6-group**

Assign an interface to a VRRP group.

**Syntax**

```
vrrp-ipv6-group vrid
```

**Parameters**

- **vrid**
  
  Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.

**Defaults**

Not configured.

**Command Modes**

INTERFACE

**Command History**

This guide is platform-specific. For command information about other platforms, see the relevant Dell Networking OS Command Line Reference Guide.

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.10(0.0)</td>
<td>Introduced on the S6100-ON.</td>
</tr>
<tr>
<td>9.8(1.0)</td>
<td>Introduced on the Z9100-ON.</td>
</tr>
<tr>
<td>9.8(0.0P5)</td>
<td>Introduced on the S4048-ON.</td>
</tr>
<tr>
<td>9.8(0.0P2)</td>
<td>Introduced on the S3048-ON.</td>
</tr>
<tr>
<td>9.7(0.0)</td>
<td>Introduced on the S6000-ON.</td>
</tr>
<tr>
<td>9.2(1.0)</td>
<td>Introduced on the Z9500.</td>
</tr>
<tr>
<td>8.4.2.1</td>
<td>The range of valid VRID values on the E-Series when VRF microcode is loaded in CAM changed from 1 to 15.</td>
</tr>
</tbody>
</table>
### Version Description

- **8.4.1.0**: Introduced on the E-Series, C-Series, and S-Series.
- **8.3.19.0**: Introduced on the S4820T.
- **8.3.7.0**: Introduced on the S4810.
- **8.3.2.0**: Introduced on the E-Series.

### Usage Information

The VRRP group only becomes active and sends VRRP packets when you configure a link-local virtual IP address. When you delete the virtual address, the VRRP group stops sending VRRP packets.

- When you do not load the VRF microcode in the CAM, the VRID for a VRRP group is the same as the VRID number configured with the `vrrp-group` or `vrrp-ipv6-group` commands.
- When you load the VRF microcode in the CAM, the VRID for a VRRP group equals 16 times the `vrrp-group` or `vrrp-ipv6-group vrid` number, plus the `ip vrf vrf-id` number. For example, if you load the VRF microcode and you configure the VRRP group as 10 in VRF 2, the VRID 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:** For all routers to interoperate, configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group.

### Related Commands

- **virtual-address**: assigns up to 12 virtual IP addresses per VRRP group.